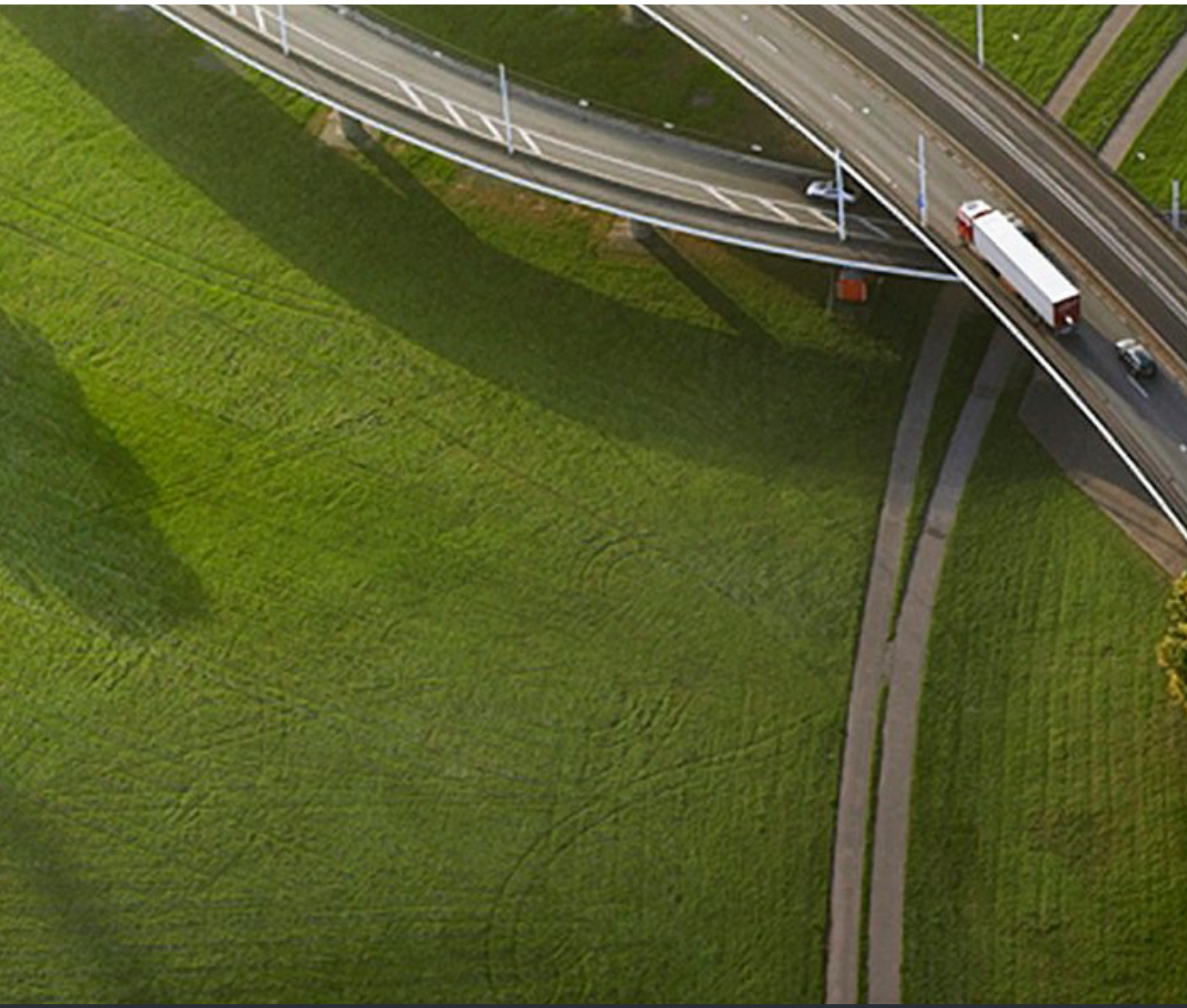
UNIFY Harmonize your enterprise



OpenScape Business V1

Administatordokumentation

A31003-P3010-M100-29-A9

Unser Qualitäts- und Umweltmanagementsystem ist entsprechend den Vorgaben der ISO9001 und ISO14001 implementiert und durch ein externes Zertifizierungsunternehmen zertifiziert.

Copyright © Unify GmbH & Co. KG 06/2015
Hofmannstr. 63, 81379 München/Deutschland

Alle Rechte vorbehalten.

Sachnummer: A31003-P3010-M100-29-A9

Die Informationen in diesem Dokument enthalten lediglich allgemeine Beschreibungen bzw. Leistungsmerkmale, die je nach Anwendungsfall nicht immer in der beschriebenen Form zutreffen oder sich durch Weiterentwicklung der Produkte ändern können. Eine Verpflichtung, die jeweiligen Merkmale zu gewährleisten besteht nur, sofern diese ausdrücklich vertraglich zugesichert wurden.

Liefermöglichkeiten und technische Änderungen vorbehalten.

Unify, OpenScape, OpenStage und HiPath sind eingetragene Warenzeichen der Unify GmbH & Co. KG. Alle anderen Marken-, Produkt- und Servicenamen sind Warenzeichen oder eingetragene Warenzeichen ihrer jeweiligen Inhaber.

UNIFY Harmonize your enterprise

unify.com

Inhalt

1 Einführung und wichtige Hinweise 39
1.1 Über diese Dokumentation 39
1.1.1 Dokumentationen und Zielgruppen 40
1.1.2 Gliederung Administratordokumentation 42
1.1.3 Gliederung Servicedokumentation 43
1.1.4 Arten von Themen 45
1.1.5 Darstellungskonventionen 45
1.2 Sicherheits- und Warnhinweise 45
1.2.1 Warnhinweise: Gefahr 47
1.2.2 Warnhinweise: Warnung 47
1.2.3 Warnhinweise: Vorsicht 48
1.2.4 Warnhinweise: Hinweis 50
1.2.5 Länderspezifische Sicherheitshinweise 51
1.2.5.1 Sicherheitshinweise für Australien 51
1.2.5.2 Sicherheitshinweise für Brasilien 52
1.2.5.3 Sicherheitshinweise für USA 52
1.2.5.4 Sicherheitshinweise für Kanada 54
1.3 Wichtige Hinweise 55
1.3.1 Verhalten in Notfällen 56
1.3.2 Bestimmungsgemäßer Gebrauch 57
1.3.3 Sachgemäße Entsorgung und Recycling 57
1.3.4 Normen und Richtlinien bezüglich der Installation 58
1.3.4.1 Anschluss von OpenScape Business X an den Versorgungsstromkreis 58
1.3.4.2 Anschluss von OpenScape Business S und OpenScape Business UC Booster Server an den Versorgungsstromkreis 58
1.3.4.3 Geschirmte Verkabelung für LAN- und WAN-Anschlüsse von OpenScape Business X 59
1.3.4.4 Brandschutzanforderungen 60
1.3.4.5 Blitzschutzanforderungen 60
1.3.4.6 Kennzeichnungen für OpenScape Business X 61
1.3.5 Hinweise zu Störaussendung und Funkstörung von OpenScape Business X 61
1.3.6 Datenschutz und Datensicherheit 61
1.3.7 Technische Vorschriften und Konformität von OpenScape Business X 62
1.3.7.1 CE-Konformität 62
1.3.7.2 Konformität mit US- und kanadischen Normen 63
1.3.7.3 Konformität mit internationalen Normen 63
1.3.8 Betriebsbedingungen 63
1.3.8.1 Betriebsbedingungen OpenScape Business X 63
1.3.8.2 Betriebsbedingungen OpenScape Business S und OpenScape Business UC Booster Server . . 64

2 Systemüberblick 65
2.1 Highlights 65
2.2 Unified Communications 66
2.2.1 UC-Funktionen (Überblick) 66
2.2.2 Benutzerzugriff auf UC-Funktionen (UC Clients) 73
2.2.3 Integration in Geschäftsanwendungen 77

2.3 OpenScape Business Modelle 78
2.3.1 Vertriebliche Ausbaustufen 78
2.3.2 UC Hardware Modelle 81
2.3.3 UC Booster Hardware 82
2.3.4 UC Software Modelle (Softswitch) 83
2.3.5 Aufbau und Umweltbedingungen 83
2.3.6 Unterstützte Telefone 83
2.4 Weiterführende Informationen 84
2.4.1 Unterstützte Sprachen 85
2.4.2 Internet-Links 87

3 Administrationskonzept 88
3.1 OpenScape Business Assistant (WBM) 88
3.1.1 Voraussetzungen für das WBM 88
3.1.2 Startseite des WBM 88
3.1.3 Einführung in das WBM 90
3.1.3.1 Wie Sie sich am WBM anmelden 92
3.1.3.2 Wie Sie sich vom WBM abmelden 92
3.1.4 Benutzerverwaltung des WBM 93
3.1.4.1 Wie Sie einen Administrator hinzufügen 95
3.1.4.2 Wie Sie Administratordaten ändern 95
3.1.4.3 Wie Sie das Administratorpasswort ändern 95
3.1.4.4 Wie Sie einen Administrator löschen 96
3.1.5 Wizards 96
3.1.5.1 Wizards – Grundinstallation 96
3.1.5.2 Wizards – Netzwerk / Internet 97
3.1.5.3 Wizards – Endgeräte / Teilnehmer 97
3.1.5.4 Wizards – Zentrale Telefonie 98
3.1.5.5 Wizards – User-Telefonie 98
3.1.5.6 Wizards – Sicherheit 99
3.1.5.7 Wizards – UC Smart (nur mit UC Smart) 99
3.1.5.8 Wizards – UC Suite (nur mit UC Suite) 99
3.1.6 Service-Center 100
3.1.6.1 Service Center – Dokumente 100
3.1.6.2 Service Center – Software 101
3.1.6.3 Service-Center – Inventory 101
3.1.6.4 Service-Center – Software-Update 101
3.1.6.5 Service-Center – Email-Weiterleitung 102
3.1.6.6 Service-Center – Remote-Zugang 102
3.1.6.7 Service-Center – Restart / Reload 102
3.1.6.8 Service-Center – Diagnose > Status 102
3.1.6.9 Service-Center – Diagnose > Event Viewer 102
3.1.6.10 Service-Center – Diagnose > Trace 102
3.1.7 Experten-Modus 103
3.1.8 Online-Hilfe 103
3.1.8.1 Wie Sie die Online-Hilfe kontextsensitiv aufrufen 103
3.2 Manager E 103
3.2.1 Wie Sie den KDS in den Manager E laden 105
3.2.2 Wie Sie den KDS in das System zurücksichern 105

4 Erstinstallation OpenScape Business X 106
4.1 Voraussetzungen für die Erstinstallation 106
4.2 Komponenten 107
4.3 Rufnummernplan 109
4.4 IP-Adressen-Schema 110
4.5 Erstinbetriebnahme 112
4.5.1 Wie Sie das Kommunikationssystem starten 113
4.5.2 Wie Sie den Admin-PC mit dem Kommunikationssystem verbinden 113
4.5.3 Wie Sie das WBM starten 114
4.6 Integration ins Kunden-LAN 116
4.6.1 Wie Sie den Wizard Erstinstallation starten 117
4.6.2 Systemeinstellungen 117
4.6.2.1 Wie Sie das Display-Logo und die Produktbezeichnung festlegen 118
4.6.2.2 Wie Sie die IP-Adressen festlegen (optional) 118
4.6.3 DHCP-Einstellungen 120
4.6.3.1 Wie Sie den internen DHCP-Server deaktivieren 120
4.6.3.2 Wie Sie den internen DHCP-Server aktivieren und konfigurieren 121
4.6.4 Länder- und Zeiteinstellungen 122
4.6.4.1 Wie Sie das Länderkennzeichen und die Sprache für Event-Logs auswählen 123
4.6.4.2 Wie Sie die DECT-Systemkennung eingeben 124
4.6.4.3 Wie Sie Datum und Uhrzeit manuell einstellen 124
4.6.4.4 Wie Sie Datum und Uhrzeit von einem SNTP-Server beziehen 125
4.6.5 UC-Lösung 125
4.6.5.1 Wie Sie die UC-Lösung festlegen 126
4.6.6 Anschluss des Kommunikationssystems ans Kunden-LAN 127
4.6.6.1 Wie Sie das Kommunikationssystem ans Kunden-LAN anschließen 127
4.7 Basiskonfiguration 127
4.7.1 Wie Sie den Wizard Basisinstallation starten 128
4.7.2 Systemrufnummern und Vernetzung 128
4.7.2.1 Wie Sie die Systemrufnummern für einen Anlagenanschluss eingeben 129
4.7.2.2 Wie Sie die Systemrufnummern für einen Mehrgeräteanschluss eingeben 130
4.7.2.3 Wie Sie die Vernetzung aktivieren oder deaktivieren 131
4.7.3 Teilnehmerdaten 131
4.7.3.1 Wie Sie die Teilnehmerdaten anzeigen 133
4.7.3.2 Wie Sie alle Rufnummern löschen 133
4.7.3.3 Vorkonfigurierte Rufnummern an den individuellen Rufnummernplan anpassen 134
4.7.3.4 Wie Sie die Teilnehmerdaten über eine XML-Datei importieren 134
4.7.4 ISDN-Konfiguration 135
4.7.4.1 Wie Sie den Anschluss von ISDN-Teilnehmern konfigurieren 135
4.7.4.2 Wie Sie den ISDN-Anlagenanschluss konfigurieren 136
4.7.4.3 Wie Sie den ISDN-Mehrgeräteanschluss konfigurieren 136
4.7.4.4 Wie Sie die ISDN-Konfiguration deaktivieren 137
4.7.5 Internet-Zugang 137
4.7.5.1 Wie Sie den Internet-Zugang über einen externen Internet-Router über den LAN-Anschluss konfigurieren 139
4.7.5.2 Wie Sie den Internet-Zugang über einen externen Internet-Router über den WAN-Anschluss konfigurieren 140
4.7.5.3 Wie Sie den Internet-Zugang über einen vorkonfigurierten ISP konfigurieren 141
4.7.5.4 Wie Sie den Internet-Zugang über den Standard-ISP PPPoE konfigurieren 143
4.7.5.5 Wie Sie den Internet-Zugang über einen Standard-ISP PPTP konfigurieren 146
4.7.5.6 Wie Sie den Internet-Zugang deaktivieren 149

4.7.6 Internet-Telefonie 149
4.7.6.1 Wie Sie einen vordefinierten ITSP konfigurieren 151
4.7.6.2 Wie Sie die Internet-Telefonie deaktivieren 157
4.7.7 Teilnehmer 157
4.7.7.1 Wie Sie ISDN-Teilnehmer konfigurieren 158
4.7.7.2 Wie Sie analoge Teilnehmer konfigurieren 160
4.7.7.3 Wie Sie UP0-Teilnehmer konfigurieren 163
4.7.7.4 Wie Sie DECT-Teilnehmer konfigurieren 165
4.7.7.5 Wie Sie IP- und SIP-Teilnehmer konfigurieren 168
4.7.8 Konfiguration von UC Suite (nur mit UC Booster Card) 171
4.7.8.1 Wie Sie UC Suite konfigurieren 171
4.7.9 Konfiguration der UC Smart Sprachboxen (nur mit UC Smart) 172
4.7.9.1 Wie Sie die UC Smart Sprachboxen konfigurieren 172
4.7.10 Konferenz-Server-Einstellungen (nur mit UC Suite) 173
4.7.10.1 Wie Sie die Konferenz-Server-Einstellungen ändern 173
4.7.11 E-Mail-Versand (optional) 173
4.7.11.1 Wie Sie den E-Mail-Versand konfigurieren 174
4.8 Abschließende Tätigkeiten 175
4.8.1 Wie Sie den Remote Service SSDP einschalten 176
4.8.2 Wie Sie die Lizenzen aktivieren und zuordnen 176
4.8.3 Wie Sie die UC Suite Clients zur Installation bereitstellen 179
4.8.4 Wie Sie den UC Smart Client zur Installation bereitstellen 180
4.8.5 Wie Sie die Datensicherung durchführen 181
4.9 Inbetriebnahme der IP-Telefone 182
4.9.1 Wie Sie ein IP-Telefon konfigurieren 183
4.9.2 Wie Sie ein SIP-Telefon konfigurieren 185

5 Erstinstallation OpenScape Business S 188
5.1 Voraussetzungen für die Erstinstallation 188
5.2 Komponenten 191
5.3 IP-Adressen-Schema 192
5.4 Rufnummernplan 192
5.5 Installation der Kommunikationssoftware 193
5.5.1 Wie Sie die Kommunikationssoftware installieren 195
5.6 Funktionskontrolle mit dem OpenScape Observer 197
5.6.1 Wie Sie den OpenScape Observer auf den PC kopieren 197
5.6.2 Wie Sie den OpenScape Observer vom PC starten 199
5.7 Inbetriebnahme 200
5.7.1 Wie Sie den Wizard Erstinstallation starten 200
5.7.2 Systemeinstellungen 200
5.7.2.1 Wie Sie das Display-Logo und die Produktbezeichnung festlegen 201
5.7.2.2 Wie Sie das Länderkennzeichen und die Sprache für Event-Logs auswählen 201
5.7.2.3 Wie Sie einen weiteren LAN-Anschluss als WAN-Schnittstelle aktivieren 202
5.8 Basiskonfiguration 203
5.8.1 Wie Sie den Wizard Basisinstallation starten 203
5.8.2 Systemrufnummern und Vernetzung 203
5.8.2.1 Wie Sie die Systemrufnummern für einen Anlagenanschluss eingeben 204
5.8.2.2 Wie Sie die Systemrufnummern für einen Mehrgeräteanschluss eingeben 205
5.8.2.3 Wie Sie die Vernetzung aktivieren oder deaktivieren 206
5.8.3 Teilnehmerdaten 206
5.8.3.1 Wie Sie die Teilnehmerdaten anzeigen 208
5.8.3.2 Wie Sie alle Rufnummern löschen 208

5.8.3.3 Vorkonfigurierte Rufnummern an den individuellen Rufnummernplan anpassen . . . 209
5.8.3.4 Wie Sie die Teilnehmerdaten über eine XML-Datei importieren . . . 209
5.8.4 Internet-Telefonie . . . 210
5.8.4.1 Wie Sie einen vordefinierten ITSP konfigurieren . . . 211
5.8.4.2 Wie Sie die Internet-Telefonie deaktivieren . . . 218
5.8.5 Teilnehmer . . . 218
5.8.5.1 Wie Sie IP- und SIP-Teilnehmer konfigurieren . . . 219
5.8.6 Konfiguration von UC Suite . . . 221
5.8.6.1 Wie Sie UC Suite konfigurieren . . . 222
5.8.7 Konferenz-Server-Einstellungen (nur mit UC Suite) . . . 222
5.8.7.1 Wie Sie die Konferenz-Server-Einstellungen ändern . . . 222
5.8.8 E-Mail-Versand (optional) . . . 223
5.8.8.1 Wie Sie den E-Mail-Versand konfigurieren . . . 223
5.9 Abschließende Tätigkeiten . . . 225
5.9.1 Wie Sie den Remote Service SSDP einschalten . . . 226
5.9.2 Wie Sie die Lizenzen aktivieren und zuordnen . . . 226
5.9.3 Wie Sie die UC Suite Clients zur Installation bereitstellen . . . 228
5.9.4 Wie Sie die Datensicherung durchführen . . . 230
5.10 Inbetriebnahme der IP-Telefone . . . 230
5.10.1 Wie Sie ein IP-Telefon konfigurieren . . . 232
5.10.2 Wie Sie ein SIP-Telefon konfigurieren . . . 233
5.11 Deinstallation der Kommunikationssoftware . . . 235
5.11.1 Wie Sie die Kommunikationssoftware deinstallieren . . . 235
5.12 Verwendete Ports . . . 235

6 Erstinstallation OpenScape Business UC Booster . . . 238
6.1 Voraussetzungen für die Erstinstallation . . . 240
6.2 Sicherung der Konfigurationsdaten des Kommunikationssystems . . . 243
6.2.1 Wie Sie die Datensicherung durchführen . . . 243
6.3 Inbetriebnahme UC Booster Card . . . 244
6.3.1 Montage der UC Booster Card . . . 244
6.3.2 Konfiguration der UC Booster Card . . . 244
6.3.3 Software-Update für die UC Booster Card . . . 245
6.3.3.1 Wie Sie ein Software-Update durchführen . . . 245
6.4 Inbetriebnahme UC Booster Server . . . 246
6.4.1 Installation der Kommunikationssoftware . . . 246
6.4.1.1 Wie Sie die Kommunikationssoftware installieren . . . 247
6.4.2 Funktionskontrolle mit dem OpenScape Observer . . . 249
6.4.2.1 Wie Sie den OpenScape Observer auf den PC kopieren . . . 250
6.4.2.2 Wie Sie den OpenScape Observer vom PC starten . . . 251
6.4.3 Konfiguration des UC Booster Servers . . . 252
6.4.3.1 IP-Adresse des Kommunikationssystems bekannt geben . . . 253
6.4.4 Software-Update für den UC Booster Server . . . 255
6.5 Basiskonfiguration . . . 255
6.6 Abschließende Tätigkeiten . . . 256
6.7 Deinstallation der Kommunikationssoftware . . . 257
6.7.1 Wie Sie die Kommunikationssoftware deinstallieren . . . 257
6.8 Hochrüstung von UC Booster Card auf UC Booster Server . . . 257
6.9 Verwendete Ports . . . 259

7 Lizenzierung 261
7.1 Lizenzierungsverfahren 262
7.2 Lizenzen 263
7.2.1 Basislizenz 265
7.2.2 Teilnehmer-Lizenzen 265
7.2.3 User-orientierte Lizenzen 266
7.2.4 Systemlizenzen 268
7.2.5 Evaluierungslizenzen 271
7.2.6 Migrations-Lizenzen 272
7.2.7 Vorschläge für Lizenzkombinationen 272
7.3 Lizenzierung eines Kommunikationssystems (Standalone) 275
7.3.1 Lizenzaktivierung (Standalone) 275
7.3.1.1 Wie Sie Lizenzen online aktivieren (Standalone) 277
7.3.1.2 Wie Sie Lizenzen offline aktivieren (Standalone) 277
7.3.2 Lizenzzuordnung (Standalone) 278
7.3.2.1 Wie Sie Teilnehmer lizenzieren (Standalone) 281
7.3.2.2 Wie Sie Leitungen lizenzieren (Standalone) 283
7.4 Lizenzierung mehrerer Kommunikationssysteme (Netzverbund) 283
7.4.1 Lizenzaktivierung (Netzverbund) 285
7.4.1.1 Wie Sie Lizenzen offline aktivieren (Netzverbund) 286
7.4.1.2 Wie Sie Lizenzdateien zu einer Netzwerklizenzdatei zusammenführen 288
7.4.2 Lizenzzuordnung (Netzverbund) 289
7.4.2.1 Wie Sie Teilnehmer lizenzieren (Netzverbund) 292
7.4.2.2 Wie Sie Leitungen lizenzieren (Netzverbund) 294
7.4.2.3 Wie Sie Systemlizenzen einem Knoten zuordnen 294
7.4.2.4 Wie Sie die Systemlizenz "Networking" einem Knoten zuordnen 295
7.5 Lizenzinformationen 295
7.5.1 Lizenzinformationen ohne Netzverbund (Standalone) 296
7.5.1.1 Wie Sie Lizenzinformationen anzeigen 296
7.5.2 Lizenzinformationen im Netzverbund 297
7.5.2.1 Wie Sie alle Lizenzen des Netzverbundes anzeigen 297
7.5.2.2 Wie Sie die an einen Knoten gebundenen Lizenzen anzeigen 298
7.5.2.3 Wie Sie alle im Netzverbund gemeinsam genutzten Lizenzen anzeigen 298
7.5.2.4 Wie Sie Teilnehmer- und User-orientierte Lizenzen knotenabhängig anzeigen 299
7.6 Lizenzprofilzuordnung 299
7.6.1 Wie Sie ein Lizenzprofil hinzufügen 300
7.6.2 Wie Sie ein Lizenzprofil bearbeiten 301
7.6.3 Wie Sie Teilnehmern ein Lizenzprofil zuordnen 302
7.6.4 Wie Sie ein Lizenzprofil löschen 303
7.7 Rehost nach Hardwaretausch 304
7.7.1 Wie Sie einen Rehost nach einem Hardwaretausch ausführen 305
7.8 Lizenzserver (Central License Server, CLS) 305
7.8.1 Wie Sie die IP-Adresse des Lizenzservers abfragen oder ändern 306
7.9 Lizenzagent (Customer License Agent, CLA) 306
7.9.1 Wie Sie eine Verbindung zum lokalen Lizenzagenten konfigurieren 307
7.9.2 Wie Sie die Verbindung zum zentralen Lizenzagenten ändern 307
7.10 Locking ID und Advanced Locking ID 307
7.10.1 Wie Sie die Locking ID des Kommunikationssystems abfragen 308
7.10.2 Wie Sie die Locking ID des Soft Switches abfragen 309
7.10.3 Wie Sie die Advanced Locking ID des Soft Switches abfragen 309

8 Integration ins interne Datennetz (LAN) 310
8.1 LAN-Schnittstelle 310
8.1.1 IP-Adresse und Netzmaske der LAN-Schnittstelle 310
8.1.1.1 Wie Sie IP-Adresse und Netzmaske der Hardware-Plattform ändern 311
8.1.1.2 Wie Sie IP-Adresse der UC Booster Card ändern 312
8.1.1.3 Wie Sie IP-Adresse und Netzmaske des Softswitches ändern 312
8.1.2 Interner IP-Adressbereich der LAN-Schnittstelle 313
8.1.2.1 Wie Sie den internen IP-Adressbereich der Hardware-Plattform ändern 313
8.1.2.2 Wie Sie den internen IP-Adressbereich der Hardware-Plattform zurücksetzen 314
8.2 DHCP 315
8.2.1 DHCP-Relay-Agent 315
8.2.1.1 Wie Sie die Hardware-Plattform als DHCP-Relay-Agent konfigurieren 315
8.2.2 DHCP-Server 316
8.2.2.1 Wie Sie den DHCP-Server der Hardware-Plattform aktivieren und konfigurieren 317
8.2.2.2 Wie Sie den DHCP-Server der Hardware-Plattform deaktivieren 319
8.2.2.3 Wie Sie den DHCP-Server des Softswitches aktivieren und konfigurieren 320
8.2.2.4 Wie Sie den DHCP-Server des Softswitches deaktivieren 321
8.3 DNS - Namensauflösung 321
8.3.1 Wie Sie einen externen DNS-Server festlegen 323
8.4 IP-Routing 323
8.4.1 Wie Sie den Default Router aktivieren oder deaktivieren 324
8.4.2 Wie Sie eine statische Route hinzufügen 324
8.4.3 Wie Sie statische Routen löschen 325
8.5 Deployment Service (DLI und DLS) 326
8.5.1 Wie Sie einen externen DLS-Server im internen DHCP-Server konfigurieren 328
8.5.2 Wie Sie den internen DLI aktivieren 329
8.5.3 Wie Sie das Kommunikationssystem als Deployment und Licensing Client konfigurieren 329

9 Anbindung an Service-Provider 331
9.1 Internet-Zugang 331
9.1.1 Internet-Zugang über externen Internet-Router 333
9.1.1.1 Wie Sie den Internet-Zugang über einen externen Internet-Router über den LAN-Anschluss konfigurieren 334
9.1.1.2 Wie Sie den Internet-Zugang über einen externen Internet-Router über den WAN-Anschluss konfigurieren 334
9.1.2 Internet-Zugang über Internet-Modem 336
9.1.2.1 Wie Sie den Internet-Zugang über einen vorkonfigurierten ISP konfigurieren 337
9.1.2.2 Wie Sie den Internet-Zugang über einen Standard-ISP PPPoE konfigurieren 339
9.1.2.3 Wie Sie den Internet-Zugang über einen Standard-ISP PPTP konfigurieren 342
9.1.3 WAN-Schnittstelle 345
9.1.4 DynDNS 345
9.1.4.1 Wie Sie den DynDNS-Service konfigurieren 346
9.1.4.2 Wie Sie den Mail-Exchanger definieren 349
9.2 Amtszugang über ITSP 350
9.2.1 Konfiguration eines ITSP 351
9.2.1.1 Wie Sie einen vordefinierten ITSP konfigurieren 353
9.2.1.2 Wie Sie einen neuen ITSP hinzufügen 359
9.2.1.3 Wie Sie eine vorkonfigurierte ITSP-Vorlage als neue Vorlage abspeichern 365
9.2.1.4 Wie Sie eine vorkonfigurierte ITSP-Vorlage anpassen 366
9.2.1.5 Wie Sie eine vorkonfigurierte ITSP-Vorlage manuell aktualisieren 367
9.2.2 STUN, Simple Traversal of UDP through NAT 367
9.2.2.1 Wie Sie den STUN-Modus festlegen 368

9.3 Amtszugang über digitale und analoge Leitungen 369
9.3.1 Leitungen 369
9.3.1.1 Wie Sie den ISDN-Amtszugang konfigurieren 370
9.3.1.2 Wie Sie einen analogen Amtszugang konfigurieren 371
9.3.1.3 Wie Sie alle Leitungen anzeigen 373
9.3.1.4 Wie Sie eine einzelne Leitung anzeigen 373
9.3.1.5 Wie Sie eine Leitungskennzahl ändern 373
9.3.1.6 Wie Sie eine MSN einer Leitung zuweisen 374
9.3.1.7 Wie Sie das ISDN-Protokoll ändern 374
9.3.1.8 Wie Sie den B-Kanal-Belegungsmodus ändern 375
9.3.1.9 Wie Sie das Wahlverfahren ändern 375
9.3.2 Richtungen 375
9.3.2.1 Wie Sie die Richtungszuordnung ändern 379
9.3.2.2 Wie Sie den Richtungsnamen ändern 379
9.3.2.3 Wie Sie die Richtungskennzahl ändern 379
9.3.2.4 Wie Sie eine Überlaufrichtung bei deaktiviertem LCR konfigurieren 380
9.3.2.5 Wie Sie eine Überlaufrichtung bei aktiviertem LCR konfigurieren 380
9.3.2.6 Wie Sie die Belegungsart konfigurieren 380
9.3.2.7 Wie Sie die Anlagenrufnummer kommend und gehend eintragen 381
9.3.2.8 Wie Sie das Format der übermittelten Rufnummer konfigurieren 381
9.3.2.9 Wie Sie die Art der übermittelten Rufnummer konfigurieren 382
9.3.2.10 Wie Sie das Richtungs-Präfix konfigurieren 382
9.3.2.11 Wie Sie eine Richtung für die Vernetzung definieren und eine zweite Amtskennziffer eintragen . . 383
9.3.3 Wähltonüberwachung 383
9.3.3.1 Wie Sie die Verzögerungszeit der Wähltonüberwachung konfigurieren 385
9.3.3.2 Wie Sie die Wähltonüberwachungszeit konfigurieren 385
9.3.3.3 Wie Sie die Ziffernwahlzeit konfigurieren 386
9.3.3.4 Wie Sie die Auswertung des zweiten Wähltons aktivieren oder deaktivieren 387
9.4 Priorisierung der Amtsholung bei aktiviertem LCR 387
9.4.1 Wie Sie die Amtsholung priorisieren 387

10 Teilnehmer 389
10.1 Rufnummernplan 389
10.1.1 Standard-Rufnummernplan 390
10.1.2 Individueller Rufnummernplan 391
10.1.2.1 Wie Sie Standard-Rufnummern löschen oder ändern 392
10.1.2.2 Wie Sie spezielle Standard-Rufnummern ändern 392
10.1.2.3 Wie Sie Rufnummern und Teilnehmerdaten importieren 393
10.2 Anforderungen an die LAN-Telefonie 394
10.2.1 Audio-Codecs 395
10.2.1.1 Wie Sie Audio-Codec-Parameter konfigurieren 396
10.2.1.2 Wie Sie Audio-Codec-Parameter einem Ziel zuordnen 397
10.2.2 Übertragung von Tönen nach RFC2833 397
10.2.2.1 Wie Sie die Übertragung von Fax- und Modem-Tönen nach RFC2833 aktivieren oder deaktivieren 397
10.2.2.2 Wie Sie die Übertragung von DTMF-Tönen nach RFC2833 aktivieren oder deaktivieren 398
10.2.3 Quality of Service 399
10.2.3.1 Wie Sie Quality of Service konfigurieren 401
10.3 IP-Teilnehmer 402
10.4 SIP-Teilnehmer 403
10.5 UP0-Teilnehmer 406
10.6 DECT-Teilnehmer 406

10.7 ISDN-Teilnehmer . . . 407
10.7.1 Wie Sie die S_0-Schnittstelle für ISDN-Teilnehmer konfigurieren . . . 409
10.7.2 Wie Sie nur eingerichtete Nummern für MSN zulassen . . . 410
10.8 Analoge Teilnehmer . . . 411
10.9 Virtuelle Teilnehmer . . . 413
10.10 Tastenprogrammierung . . . 413
10.10.1 Wie Sie die Funktionstasten der Systemtelefone programmieren . . . 414
10.11 Teilnehmer-Profile . . . 416
10.12 Konfiguration der Teilnehmer . . . 416
10.12.1 Wie Sie IP-Teilnehmer konfigurieren . . . 418
10.12.2 Wie Sie SIP-Teilnehmer konfigurieren . . . 422
10.12.3 Wie Sie UP0-Teilnehmer konfigurieren . . . 426
10.12.4 Wie Sie DECT-Teilnehmer konfigurieren . . . 429
10.12.5 Wie Sie ISDN-Teilnehmer konfigurieren . . . 432
10.12.6 Wie Sie analoge Teilnehmer konfigurieren . . . 435
10.12.7 Wie Sie den Namen der Teilnehmer ändern . . . 438
10.13 Konfiguration der Teilnehmer-Profile . . . 439
10.13.1 Wie Sie ein neues Teilnehmer-Profil anlegen . . . 440
10.13.2 Wie Sie Teilnehmer-Profile und deren Mitglieder anzeigen . . . 441
10.13.3 Wie Sie Mitglieder zu einem Teilnehmer-Profil hinzufügen . . . 441
10.13.4 Wie Sie Mitglieder aus einem Teilnehmer-Profil löschen . . . 442
10.13.5 Wie Sie ein einzelnes Teilnehmer-Profil exportieren oder importieren . . . 443
10.13.6 Wie Sie die Werte und Einstellungen eines Teilnehmer-Profils ändern . . . 444
10.13.7 Wie Sie alle Teilnehmer-Profile exportieren oder importieren . . . 445
10.14 Konfiguration der Authentifizierungsdaten am SIP-Telefon . . . 446
10.14.1 Wie Sie die Authentifizierungsdaten über das WBM des SIP-Telefons konfigurieren . . . 446
10.14.2 Wie Sie die Authentifizierungsdaten am Display des SIP-Telefons konfigurieren . . . 449
10.15 Export von Teilnehmerdaten . . . 450
10.15.1 Wie Sie die Teilnehmerdaten exportieren . . . 450

11 UC Smart . . . 451
11.1 Grundeinstellungen für UC Smart . . . 451
11.1.1 Wie Sie UC Smart aktivieren . . . 451
11.1.2 Wie Sie UC Smart konfigurieren . . . 452
11.1.3 Wie Sie die IP-Adressen von Komponenten des Systems ermitteln . . . 453
11.1.4 Wie Sie den Status von UC Smart ermitteln . . . 453
11.2 UC Smart Clients . . . 453
11.2.1 myPortal Smart . . . 454
11.2.2 myPortal for OpenStage (UC Smart) . . . 454
11.2.3 Voraussetzungen für myPortal Smart . . . 455
11.2.4 Voraussetzungen für myPortal for OpenStage (UC Smart) . . . 456
11.3 Benutzer von UC Smart . . . 456
11.3.1 Wie Sie einen Benutzer von UC Smart konfigurieren . . . 457
11.3.2 Wie Sie für einen Benutzer von UC Smart das Kennwort ändern . . . 458
11.4 Anwesenheitsstatus (UC Smart) . . . 459
11.5 Verzeichnisse und Journal (UC Smart) . . . 459
11.5.1 Verzeichnisse (UC Smart) . . . 459
11.5.1.1 Wie Sie Verzeichnisse für Systemtelefone konfigurieren (UC Smart) . . . 460
11.5.2 Internes Verzeichnis (UC Smart) . . . 461
11.5.2.1 Wie Sie die Anzeige eines Teilnehmers im internen Verzeichnis aktivieren oder deaktivieren 461
11.5.3 Favoritenliste (UC Smart) . . . 462
11.5.4 Systemtelefonbuch (UC Smart) . . . 462
11.5.5 Journal (UC Smart) . . . 462

11.6 Anrufe (UC Smart) 463
11.6.1 Rufnummernformate 463
11.7 Konferenzen (UC Smart) 464
11.7.1 Ad-hoc-Konferenz (UC Smart) 464
11.8 Sprachbox / SmartVM (UC Smart) 465
11.8.1 Konfiguration der Sprachbox / SmartVM 467
11.8.1.1 Wie Sie die Sprachbox deaktivieren oder aktivieren 468
11.8.1.2 Wie Sie die Sprachbox / SmartVM konfigurieren 468
11.8.1.3 Wie Sie eine Standardmailbox für einen Teilnehmer hinzufügen 470
11.8.1.4 Wie Sie die Berechtigungsgruppe für einen Sprachbox-Port ändern 471
11.8.1.5 Wie Sie die Struktur des Telefonmenüs der Sprachbox ändern 471
11.8.1.6 Wie Sie einzelne Begrüßungen laden, sichern und löschen 472
11.8.1.7 Wie Sie Begrüßungen und Nachrichten sichern und wiederherstellen 472
11.8.2 Benachrichtigungsdienst für neue Nachrichten 474
11.8.2.1 Wie Sie die E-Mail-Benachrichtigung aktivieren oder deaktivieren 474
11.9 Instant Messaging (UC Smart) 475
11.9.1 Sofortnachrichten 475

12 UC Suite 476
12.1 Grundeinstellungen für UC Suite 476
12.1.1 Wie Sie UC Suite aktivieren 476
12.1.2 Wie Sie die Berechtigung von systemseitig eingeleiteten UC-Anrufe einschränken 477
12.2 UC Suite Clients 477
12.2.1 myPortal for Desktop 478
12.2.1.1 Wie Sie eine alternative moderne Benutzeroberfläche für myPortal for Desktop bereitstellen . 479
12.2.1.2 Wie Sie die alternative moderne Benutzeroberfläche für myPortal for Desktop löschen 479
12.2.2 myPortal for Outlook 480
12.2.3 Fax Printer 480
12.2.4 myAttendant 480
12.2.5 myPortal for OpenStage (UC Suite) 481
12.2.6 Voraussetzungen für UC Suite PC-Clients 481
12.2.7 Voraussetzungen für myPortal for OpenStage (UC Suite) 485
12.2.8 Silent Installation/Deinstallation für UC Suite PC-Clients 485
12.2.8.1 Wie Sie eine Silent Installation durchführen 486
12.2.8.2 Wie Sie eine Silent Deinstallation durchführen 487
12.2.9 Automatische Updates 489
12.3 Benutzer und Benutzer-Profile von UC Suite 489
12.3.1 Benutzer von UC Suite 489
12.3.1.1 Wie Sie einen Benutzer von UC Suite konfigurieren 491
12.3.1.2 Wie Sie einen Benutzer von UC Suite zurücksetzen 492
12.3.1.3 Wie Sie einen Benutzer von UC Suite als Agenten konfigurieren (myAgent) 492
12.3.1.4 Wie Sie für einen Benutzer von UC Suite den Anwesenheitsstatus ändern 493
12.3.1.5 Wie Sie für einen Benutzer von UC Suite das Kennwort ändern 494
12.3.1.6 Wie Sie für einen Benutzer von UC Suite die Kennwortlänge ändern 494
12.3.2 Benutzer-Profile von UC Suite 495
12.3.2.1 Wie Sie ein Benutzer-Profil von UC Suite hinzufügen 496
12.3.2.2 Wie Sie ein Benutzer-Profil von UC Suite ändern 496
12.3.2.3 Wie Sie die Benutzer-Profile von UC Suite anzeigen 497
12.3.2.4 Wie Sie Mitglieder zu einem Benutzer-Profil von UC Suite hinzufügen 497
12.3.2.5 Wie Sie Mitglieder aus einem Benutzer-Profil von UC Suite löschen 498
12.3.2.6 Wie Sie ein Benutzer-Profil von UC Suite löschen 498

12.4 Anwesenheitsstatus und CallMe-Dienst 498
12.4.1 Anwesenheitsstatus (UC Suite) 499
12.4.2 CallMe-Dienst 502
12.4.3 Statusbezogene Anrufumleitung 503
12.4.4 Regelbasierte Anrufumleitung 503
12.5 Verzeichnisse und Journal (UC Suite) 504
12.5.1 Verzeichnisse (UC Suite) 504
12.5.1.1 Wie Sie Verzeichnisse für Systemtelefone konfigurieren (UC Suite) 506
12.5.2 Internes Verzeichnis (UC Suite) 507
12.5.2.1 Wie Sie die Anzeige analoger Teilnehmer im internen Verzeichnis aktivieren oder deaktivieren 507
12.5.3 Externes Verzeichnis 508
12.5.3.1 Wie Sie eine CSV-Datei vom lokalen Dateisystem in das externe Verzeichnis importieren . . . 509
12.5.3.2 Wie Sie Zugriff auf eine externe Datenbank für das Externe Verzeichnis hinzufügen 510
12.5.4 Externes Offline-Verzeichnis (LDAP) 510
12.5.4.1 Wie Sie ein externes Offline-Verzeichnis (LDAP) für PC-Clients hinzufügen 512
12.5.4.2 Wie Sie ein externes Offline-Verzeichnis (LDAP) für PC-Clients löschen 513
12.5.4.3 Wie Sie ein externes Offline-Verzeichnis (LDAP) für Systemtelefone hinzufügen 513
12.5.5 Systemtelefonbuch (UC Suite) 514
12.5.6 Abteilungen 514
12.5.6.1 Wie Sie eine Abteilung hinzufügen 514
12.5.6.2 Wie Sie Teilnehmer einer Abteilung zuordnen 515
12.5.6.3 Wie Sie eine Abteilung bearbeiten 515
12.5.6.4 Wie Sie eine Abteilung entfernen 515
12.5.7 Favoritenliste 516
12.5.8 Journal (UC Suite) 516
12.5.8.1 Wie Sie die maximale Aufbewahrungsdauer für das Journal ändern 518
12.6 Anrufe (UC Suite) 518
12.6.1 Desktop-Wahl und Clipboard-Wahl 519
12.6.2 PopUp-Fenster 519
12.6.3 Aufzeichnen von Anrufen 519
12.6.3.1 Wie Sie das Aufzeichnen von Anrufen aktivieren oder deaktivieren 520
12.6.3.2 Wie Sie eine Ansage für Aufzeichnung aktivieren oder deaktivieren 520
12.6.3.3 Wie Sie den Hinweiston für eine Aufzeichnung aktivieren oder deaktivieren 521
12.7 Konferenzen (UC Suite) 521
12.7.1 Konferenzmanagement 522
12.7.1.1 Wie Sie die Einwahlnummer für einen virtuellen Konferenzraum ändern 526
12.7.1.2 Wie Sie mehrere externe Konferenzteilnehmer zulassen oder verhindern 526
12.7.1.3 Wie Sie den Konferenzton aktivieren oder deaktivieren 527
12.7.1.4 Wie Sie die Zeitspanne für automatisches Beenden von Konferenzen ändern 527
12.7.1.5 Wie Sie Details zu einer gespeicherten Konferenz abfragen 528
12.7.1.6 Wie Sie eine gespeicherte Konferenz löschen 528
12.7.1.7 Wie Sie das Aufzeichnen von Konferenzen konfigurieren 528
12.7.2 Ad-hoc-Konferenz (UC Suite) 529
12.7.3 Geplante Konferenz 529
12.7.4 Permanente Konferenz 531
12.7.5 Offene Konferenz 532
12.7.6 Web Collaboration-Einbindung 533
12.7.6.1 Wie Sie die Verbindung zum Web Collaboration Server (Custom Server) konfigurieren 535
12.7.6.2 Wie Sie die Verbindung zum Web Collaboration Server (Public Server) konfigurieren 536
12.7.6.3 Wie Sie die Verbindung zum Web Collaboration Server deaktivieren 537

12.8 Sprach- und Faxnachrichten (UC Suite) . . . 537
12.8.1 Sprachbox (UC Suite) . . . 537
12.8.1.1 Wie Sie die Rufnummer der Sprachbox (UC Suite) konfigurieren . . . 540
12.8.1.2 Wie Sie die Rufweiterschaltung zur Sprachbox (UC Suite) konfigurieren . . . 540
12.8.1.3 Wie Sie Parameter der Sprachbox (UC Suite) konfigurieren . . . 540
12.8.1.4 Wie Sie die Aufbewahrungsdauer für Sprachnachrichten (UC Suite) konfigurieren . . . 541
12.8.1.5 Wie Sie eine Info für empfangene Sprachnachrichten (UC Suite) konfigurieren . . . 542
12.8.1.6 Wie Sie die Briefkastentaste für die Abfrage von Sprachnachrichten (UC Suite) konfigurieren . . . 542
12.8.2 Ansagen der Sprachbox (UC Suite) . . . 542
12.8.2.1 Wie Sie eine Ansage für die Sprachbox (UC Suite) importieren . . . 544
12.8.2.2 Wie Sie die Sprache für Ansagen der Sprachbox (UC Suite) ändern . . . 545
12.8.3 Faxbox . . . 545
12.8.3.1 Wie Sie eine Faxbox für Teilnehmer hinzufügen . . . 546
12.8.3.2 Wie Sie den Dateityp für gespeicherte Faxnachrichten (UC Suite) konfigurieren . . . 547
12.8.4 Senden von Faxnachrichten mit Fax Printer . . . 547
12.8.4.1 Wie Sie ein zentrales Faxdeckblatt hinzufügen . . . 548
12.8.4.2 Wie Sie das zentrale Faxdeckblatt bearbeiten . . . 549
12.8.4.3 Wie Sie eine Kopfzeile für Fax Printer hinzufügen . . . 549
12.8.4.4 Wie Sie eine Kopfzeile für Fax Printer ändern . . . 550
12.8.4.5 Wie Sie eine Kopfzeile für Fax Printer löschen . . . 550
12.8.5 Benachrichtigungsdienst für neue Nachrichten (UC Suite) . . . 551
12.8.6 E-Mail-Versand . . . 551
12.8.6.1 Wie Sie den E-Mail-Versand konfigurieren . . . 552
12.8.7 SMS-Template . . . 553
12.8.7.1 Wie Sie ein SMS-Template hinzufügen . . . 554
12.8.7.2 Wie Sie ein SMS-Template bearbeiten . . . 554
12.8.7.3 Wie Sie ein SMS-Template entfernen . . . 555
12.8.8 Fax over IP (T.38-Fax) . . . 555
12.8.8.1 Wie Sie Fax over IP (T.38-Fax) aktivieren oder deaktivieren . . . 556
12.9 Instant Messaging (UC Suite) . . . 557
12.9.1 Sofortnachrichten (UC Suite) . . . 557
12.9.1.1 Wie Sie Sofortnachrichten (UC Suite) aktivieren oder deaktivieren . . . 558
12.10 AutoAttendant . . . 558
12.10.1 Persönlicher AutoAttendant . . . 558

13 Funktionen am Telefon . . . 560
13.1 Anrufen . . . 560
13.1.1 Ziffernwahl . . . 560
13.1.2 Blockwahl . . . 560
13.1.3 Keypad-Wahl . . . 560
13.1.4 Wahlendeerkennung . . . 561
13.1.5 Editieren der Wahl . . . 561
13.1.5.1 Wie Sie das Editieren der Wahl aktivieren oder deaktivieren . . . 562
13.1.6 Wahlwiederholung . . . 562
13.1.6.1 Wie Sie die automatische Wahlwiederholung aktivieren oder deaktivieren . . . 563
13.1.7 Kurzwahl zentral (KWZ) . . . 563
13.1.7.1 Wie Sie ein Kurzwahlziel hinzufügen . . . 565
13.1.7.2 Wie Sie Kurzwahlziele aus einer XML- oder CSV-Datei importieren . . . 565
13.1.7.3 Wie Sie Kurzwahlziele in eine XML-Datei exportieren . . . 566
13.1.7.4 Wie Sie Kurzwahlziele bearbeiten . . . 567
13.1.8 Kurzwahl individuell (KWI) . . . 567
13.1.9 Direktruf . . . 568
13.1.10 Direktansprechen / Direktantworten . . . 568

13.1.10.1 Wie Sie den Direktansprechschutz für Teilnehmer aktivieren oder deaktivieren . . . 569
13.1.11 Assoziierte Wahl . . . 570
13.1.12 Leitungsvormerken . . . 570
13.1.12.1 Wie Sie Leitungsvormerken aktivieren oder deaktivieren . . . 571
13.1.13 Privatleitung . . . 571
13.2 Anrufsignalisierung, Rufnummernanzeige . . . 572
13.2.1 Unterschiedliche Anrufsignalisierung . . . 572
13.2.2 Rufnummernübermittlung des Anrufers (CLIP) . . . 572
13.2.2.1 Wie Sie einstellbare CLIP aktivieren oder deaktivieren . . . 573
13.2.3 Rufnummernunterdrückung des Anrufers (CLIR) . . . 573
13.2.3.1 Wie Sie die Unterdrückung der Teilnehmerrufnummer aktivieren oder deaktivieren . . . 574
13.2.4 Rufnummernübermittlung des Angerufenen (COLP) . . . 575
13.2.4.1 Wie Sie die Rufnummernübermittlung des Angerufenen aktivieren oder deaktivieren . . . 575
13.2.5 Rufnummernunterdrückung des Angerufenen (COLR) . . . 575
13.2.6 CLIP no screening (Übermittlung kundenspezifischer Rufnummerninformationen) . . . 576
13.2.6.1 Wie Sie CLIP no screening konfigurieren . . . 576
13.2.7 CLIP für analoge Endgeräte . . . 577
13.2.8 Stiller Ruf / Ruhe . . . 577
13.2.9 Rufnummernumwertung in Namen bei Kurzwahl zentral . . . 577
13.3 Funktionen während der Verbindung . . . 577
13.3.1 Halten . . . 578
13.3.2 Parken . . . 578
13.3.3 Rückfrage . . . 579
13.3.4 Makeln . . . 579
13.3.5 Übergabe . . . 580
13.3.6 Wiederanruf . . . 580
13.3.7 Call Monitoring (nur ausgewählte Länder) . . . 581
13.3.7.1 Wie Sie Call Monitoring für einen Teilnehmer aktivieren oder deaktivieren . . . 582
13.3.8 Diskretes Ansprechen . . . 582
13.4 Steuern der Erreichbarkeit . . . 584
13.4.1 Rufweiterschaltung . . . 584
13.4.1.1 Wie Sie eine Rufweiterschaltung konfigurieren . . . 585
13.4.2 Anrufumleitung (AUL) . . . 588
13.4.2.1 Wie Sie Anrufumleitung über analoge Amtsleitungen aktivieren oder deaktivieren . . . 589
13.4.2.2 Wie Sie eine Anrufumleitung nach Anrufumleitung zum externernen Ziel aktivieren oder deaktivieren . . . 590
13.4.3 Anrufumleitung nach Zeit . . . 590
13.4.4 Rufweiterschaltung im Amt (nicht für USA) . . . 591
13.4.5 Rufzuordnung . . . 591
13.4.5.1 Wie Sie eine Rufzuordnung konfigurieren . . . 592
13.4.6 Rufzuschaltung . . . 592
13.4.7 Abweisen von Anrufen . . . 593
13.4.8 Zurückstellen eines Anrufs . . . 594
13.4.9 Anrufschutz . . . 594
13.5 Optimieren der Kommunikationsabläufe . . . 595
13.5.1 Rückruf . . . 595
13.5.2 Anklopfen . . . 596
13.5.2.1 Wie Sie Anklopfen aktivieren oder deaktivieren . . . 597
13.5.2.2 Wie Sie sofortiges Anklopfen durch Vermittlungsplatz aktivieren oder deaktivieren . . . 598
13.5.3 Aufschalten . . . 598
13.5.3.1 Wie Sie einen internen Teilnehmer für das Aufschalten berechtigen . . . 599
13.5.3.2 Wie Sie den Abwurfplatz für das Aufschalten berechtigen . . . 599
13.5.4 Abwesenheitstexte . . . 600

13.5.4.1 Wie Sie einen Abwesenheitstext ändern 600
13.5.5 Mitteilungstexte 600
13.5.5.1 Wie Sie einen Mitteilungstext ändern 601
13.5.6 Assoziierte Dienste 601
13.5.6.1 Wie Sie Assoziierte Dienste aktivieren oder deaktivieren 602
13.5.7 DISA. 602
13.5.7.1 Wie Sie die DISA-Berechtigung für einen Teilnehmer aktivieren oder deaktivieren. 603
13.5.7.2 Wie Sie eine DISA-Nummer konfigurieren 604
13.5.7.3 Wie Sie den DISA-Sicherheitsmodus konfigurieren 604
13.5.8 Flex Call/Mobile PIN 604
13.5.9 Relocate/Rufnummerntausch 605
13.5.9.1 Wie Sie Relocate/Rufnummertausch systemweit freigeben 606
13.5.10 Rücksetzen aktivierter Leistungsmerkmale 606
13.5.11 Prozeduren 606
13.5.12 Weckeinrichtung und Termine 608

14 Arbeiten im Team (Gruppen). 609
14.1 Anrufübernahmegruppe, Gruppenruf und Sammelanschluss 609
14.1.1 Anrufübernahmegruppe 609
14.1.2 Gruppenruf. 611
14.1.3 Sammelanschluss 615
14.1.4 Konfiguration von Anrufübernahmegruppen, Gruppenrufen und Sammelanschlüssen über Wizards 618
14.1.4.1 Wie Sie Anrufübernahmegruppen konfigurieren 619
14.1.4.2 Wie Sie ein Mitglied zur Anrufübernahmegruppe hinzufügen oder löschen 619
14.1.4.3 Wie Sie einen Gruppenruf (Gruppe) hinzufügen 620
14.1.4.4 Wie Sie einen Gruppenruf (Gruppe) ändern 621
14.1.4.5 Wie Sie einen Gruppenruf (Gruppe) löschen 623
14.1.4.6 Wie Sie ein Mitglied zum Gruppenruf (Gruppe) hinzufügen oder löschen 623
14.1.4.7 Wie Sie einen Sammelanschluss hinzufügen 624
14.1.4.8 Wie Sie einen Sammelanschluss ändern 625
14.1.4.9 Wie Sie einen Sammelanschluss löschen 626
14.1.4.10 Wie Sie ein Mitglied zum Sammelanschluss hinzufügen oder löschen 627
14.1.5 Konfiguration von Anrufübernahmegruppen, Gruppenrufen und Sammelanschlüssen über Experten-Modus. 628
14.1.5.1 Wie Sie die Anzeige der Rufnummer und des Namens des Anrufers aktivieren oder deaktivieren 628
14.1.5.2 Wie Sie den Aufmerksamkeitston aktivieren oder deaktivieren 629
14.1.5.3 Wie Sie die Anrufübernahme von Wiederanrufen aktivieren oder deaktivieren 629
14.1.5.4 Wie Sie einen Gruppenruf (Freifall oder Anklopfen) hinzufügen 630
14.1.5.5 Wie Sie einen Gruppenruf (Freifall oder Anklopfen) anzeigen oder ändern 631
14.1.5.6 Wie Sie einen Gruppenruf (Freifall oder Anklopfen) löschen 631
14.1.5.7 Wie Sie ein Mitglied zum Gruppenruf (Freifall oder Anklopfen) hinzufügen oder löschen 632
14.1.5.8 Wie Sie Anklopfschutz für Gruppenmitglied ein- oder ausschalten 632
14.2 Teamschaltung / Team-Gruppe und Chef/Sekretär / Top-Gruppe 633
14.2.1 Teamschaltung / Team-Gruppe 633
14.2.2 Chef/Sekretär / Top-Gruppe 636
14.2.3 Konfiguration von Teamschaltungen / Team-Gruppen und Chef/Sekretär-Funktionen / Top-Gruppen über Wizards 640
14.2.3.1 Wie Sie eine Teamschaltung / Team-Gruppe hinzufügen 641
14.2.3.2 Wie Sie eine Teamschaltung / Team-Gruppe ändern 642
14.2.3.3 Wie Sie eine Teamschaltung / Team-Gruppe löschen 643

14.2.3.4 Wie Sie eine Chef/Sekretär- / Top-Gruppe hinzufügen . . . 643
14.2.3.5 Wie Sie eine Chef/Sekretär- / Top-Gruppe ändern . . . 644
14.2.3.6 Wie Sie eine Chef/Sekretär- / Top-Gruppe löschen . . . 645
14.2.4 Konfiguration von Teamschaltungen / Team-Gruppen und Chef/Sekretär-Funktionen / Top-Gruppen über Experten-Modus . . . 646
14.2.4.1 Wie Sie ein Mitglied zur Teamschaltung / Team-Gruppe hinzufügen oder löschen . . . 646
14.2.4.2 Wie Sie ein Mitglied einer Teamschaltung / Team-Gruppe ändern. . . . 647
14.2.4.3 Wie Sie die Eigenschaften der Mitglieder einer Teamschaltung / Team-Gruppe ändern . . . 647
14.2.4.4 Wie Sie die Telefon-Tastenbelegung für Teamschaltung / Team-Gruppe ändern . . . 648
14.2.4.5 Wie Sie eine Faxbox zur Teamschaltung / Team-Gruppe hinzufügen . . . 648
14.2.4.6 Wie Sie ein Mitglied zur Chef/Sekretär / Top-Gruppe hinzufügen oder löschen . . . 649
14.2.4.7 Wie Sie ein Mitglied einer Chef/Sekretär / Top-Gruppe ändern . . . 649
14.2.4.8 Wie Sie die Eigenschaften der Mitglieder einer Chef/Sekretär / Top-Gruppe ändern . . . 650
14.2.4.9 Wie Sie eine Faxbox zur Chef/Sekretär / Top-Gruppe hinzufügen . . . 650
14.3 Basic-MULAP und Chef-MULAP . . . 651
14.3.1 Basic-MULAP . . . 651
14.3.2 Chef-MULAP . . . 653
14.3.3 Konfiguration von Basic-MULAPs und Chef-MULAPs . . . 656
14.3.3.1 Wie Sie Basic-MULAP hinzufügen . . . 656
14.3.3.2 Wie Sie Basic-MULAP anzeigen oder ändern . . . 657
14.3.3.3 Wie Sie Basic-MULAP löschen . . . 658
14.3.3.4 Wie Sie ein Mitglied zur Basic-MULAP hinzufügen oder löschen . . . 658
14.3.3.5 Wie Sie ein Mitglied einer Basic-MULAP ändern . . . 659
14.3.3.6 Wie Sie eine Chef-MULAP hinzufügen . . . 659
14.3.3.7 Wie Sie eine Chef-MULAP anzeigen oder ändern . . . 660
14.3.3.8 Wie Sie eine Chef-MULAP löschen . . . 660
14.3.3.9 Wie Sie ein Mitglied zur Chef-MULAP hinzufügen oder löschen . . . 661
14.3.3.10 Wie Sie ein Mitglied einer Chef-MULAP ändern . . . 661
14.4 Sprachbox-Gruppe und Faxbox-Gruppe . . . 662
14.4.1 Sprachbox-Gruppe . . . 662
14.4.2 Faxbox-Gruppe . . . 663
14.4.3 Konfiguration von Sprachbox-Gruppen und Faxbox-Gruppen . . . 663
14.4.3.1 Wie Sie eine Sprachbox-Gruppe hinzufügen . . . 664
14.4.3.2 Wie Sie eine Sprachbox-Gruppe anzeigen oder ändern . . . 664
14.4.3.3 Wie Sie eine Sprachbox-Gruppe löschen . . . 665
14.4.3.4 Wie Sie ein Mitglied zur Sprachbox-Gruppe hinzufügen oder löschen . . . 665
14.4.3.5 Wie Sie ein Mitglied einer Sprachbox-Gruppe ändern . . . 666
14.4.3.6 Wie Sie eine Faxbox-Gruppe konfigurieren . . . 666
14.4.3.7 Wie Sie eine Faxbox-Gruppe anzeigen oder ändern . . . 667
14.4.3.8 Wie Sie eine Faxbox-Gruppe löschen . . . 668
14.4.3.9 Wie Sie ein Mitglied zur Faxbox-Gruppe hinzufügen oder löschen . . . 668
14.5 Direktansprechen für Gruppen. . . . 669
14.5.1 Durchsage an Gruppe . . . 669
14.5.2 Übergabe an Gruppe aus Durchsage . . . 669
14.6 Anrufverteilung (UCD Uniform Call Distribution) . . . 670
14.6.1 Anrufverteilung / UCD-Gruppe . . . 671
14.6.1.1 Wie Sie eine Anrufverteilung / UCD-Gruppen konfigurieren . . . 672
14.6.2 UCD-Agenten . . . 673
14.6.2.1 Wie Sie UCD-Agenten hinzufügen oder löschen . . . 674
14.6.3 Nachbearbeitung . . . 675
14.6.3.1 Wie Sie die automatische Nachbearbeitungszeit ändern . . . 676
14.6.4 Priorisierte Anrufordnung . . . 676

14.6.4.1 Wie Sie die Priorisierung der Anrufordnung ändern 677
14.6.5 UCD-Anrufe automatisch annehmen 677
14.6.5.1 Wie Sie das automatische Annehmen von UCD-Anrufen ändern 678
14.6.6 UCD-Warteschlange 678
14.6.6.1 Wie Sie eine UCD-Warteschlange ändern 679
14.6.7 UCD-Überlauf 680
14.6.7.1 Wie Sie den UCD-Überlauf ändern 680
14.6.8 UCD-Nachtschaltung 681
14.6.9 Ansagen / Wartemusik bei UCD 682
14.6.9.1 Wie Sie Ansagen / Wartemusik bei UCD ändern 682
14.6.10 Übergabe an UCD-Gruppen 683
14.6.10.1 Wie Sie die Wiederanrufzeit für übergebene Gespräche an UCD-Gruppen ändern 683
14.6.11 Auslösen von UCD-Anrufen über analoge Leitungen 684
14.6.11.1 Wie Sie die Auslösezeit für UCD-Anrufe über analoge Leitungen ändern 684

15 Anruf-Routing 685
15.1 Berechtigungen (Wahlkontrolle) 685
15.1.1 Berechtigungsgruppen und Berechtigungsklassen 685
15.1.1.1 Wie Sie den Namen einer Berechtigungsgruppe ändern 686
15.1.1.2 Wie Sie die Berechtigungsklassen einer Berechtigungsgruppe ändern 686
15.1.1.3 Wie Sie alle Teilnehmer einer Berechtigungsgruppe anzeigen 687
15.1.2 Erlaubnis- und Verbotslisten 687
15.1.2.1 Wie Sie eine Notrufnummernliste erstellen 688
15.1.2.2 Wie Sie eine Erlaubnis- und eine Verbotsliste erstellen 689
15.1.2.3 Wie Sie weitere Erlaubnislisten erstellen 690
15.1.2.4 Wie Sie weitere Verbotslisten erstellen 690
15.1.2.5 Wie Sie alle Rufnummern einer Verbotsliste anzeigen 691
15.1.2.6 Wie Sie alle Rufnummern einer Erlaubnisliste anzeigen 691
15.1.2.7 Wie Sie den Auswertungsfilter für eine Verbotsliste ändern 691
15.1.3 Nachtschaltung 692
15.1.3.1 Wie Sie Berechtigungen für die manuelle Nachtschaltung vergeben 693
15.1.3.2 Wie Sie Berechtigungen für die manuelle Nachtschaltung löschen 694
15.1.3.3 Wie Sie die zeitgesteuerte Nachtschaltung konfigurieren 694
15.1.3.4 Wie Sie einen Sondertag für die zeitgesteuerte Nachtschaltung konfigurieren 695
15.1.3.5 Wie Sie einen Sondertag für die zeitgesteuerte Nachtschaltung löschen 695
15.1.4 Automatische Berechtigungsumschaltung nach Zeit 695
15.1.4.1 Zeitplan 696
15.1.5 VBZ (Verkehrsbeziehungen) 697
15.1.5.1 VBZ-Gruppen (Verkehrsbeziehungsgruppen) 698
15.1.5.2 Zuordnung der KWZ-Nummern zu VBZ-Gruppen 698
15.1.5.3 Wie Sie Teilnehmer einer VBZ-Gruppe zuweisen 699
15.1.5.4 Wie Sie die Leitung einer VBZ-Gruppe zuweisen 699
15.1.5.5 Wie Sie die VBZ-Matrix ändern 700
15.1.6 Zentrales Codeschloss, Berechtigungsumschaltung 700
15.1.7 Individuelles Codeschloss (Telefon abschließen) 701
15.1.7.1 Wie Sie das individuelle Codeschloss zurücksetzen 701
15.1.8 R-Gesprächsschutz je Amtsleitung (nur für Brasilien) 702
15.1.9 R-Gesprächsschutz je Teilnehmer (nur für Brasilien) 702
15.2 LCR (Least Cost Routing, Leitweglenkung) 702
15.2.1 LCR-Funktionalität 703
15.2.1.1 Wie Sie die LCR freigeben 705
15.2.2 LCR-Wahlplan 706

15.2.2.1 Wie Sie den Wahlplan bearbeiten . . . 707
15.2.3 LCR-Wegetabelle . . . 708
15.2.3.1 Wie Sie Wegetabellen bearbeiten . . . 709
15.2.4 LCR-Berechtigung . . . 710
15.2.4.1 Wie Sie die LCR-Berechtigung vergeben und ändern . . . 710
15.2.5 LCR-Wahlregeln . . . 710
15.2.5.1 Wie Sie Wahlregeln bearbeiten . . . 712
15.2.6 Netzanbieter . . . 713
15.2.7 Gezielte Belegung von Amtsleitungen . . . 714
15.2.7.1 Wie Sie die Kennzahl für gezielte Belegung von ISDN-Amtsleitungen konfigurieren . . . 715
15.2.7.2 Wie Sie Kennzahlen für die gezielte Amtsbelegung anzeigen . . . 715
15.3 Wahlbewertung und Call-Routing . . . 716
15.3.1 Überblick Call Routing / LCR . . . 717
15.3.2 Flußdiagramm Wahlbewertung . . . 719
15.3.3 Call Routing und LCR im Netzverbund . . . 720
15.3.3.1 Dediziertes Gateway . . . 722
15.3.4 Szenarien: Wahlbewertung und Call Routing . . . 723
15.3.4.1 Teilnehmer A ruft Teilnehmer B über Internrufnummer . . . 724
15.3.4.2 Teilnehmer A ruft Teilnehmer B über öffentliche Rufnummer . . . 726
15.3.4.3 Teilnehmer A ruft externen Teilnehmer über Amt . . . 729
15.3.4.4 ISDN-Amt ruft Teilnehmer A . . . 731
15.3.4.5 Sonderkonfigurationen . . . 733
15.3.4.6 Teilnehmer A ruft Teilnehmer C über Internrufnummer . . . 735
15.3.4.7 Teilnehmer A ruft Teilnehmer C über öffentliche Rufnummer im Netzverbund . . . 738
15.3.4.8 ISDN-Amt ruft Teilnehmer C . . . 741
15.3.4.9 ISDN-Amt Gateway 1 ruft Teilnehmer D . . . 742
15.3.4.10 Teilnehmer D ruft externen Teilnehmer über Amt . . . 746
15.4 Notrufe . . . 748
15.4.1 Röchelschaltung / Hotline . . . 750
15.4.1.1 Wie Sie einen Hotlineziel konfigurieren und ändern . . . 750
15.4.1.2 Wie Sie die Röchelzeit ändern . . . 751
15.4.1.3 Wie Sie Röcheln oder Hotline für einen Teilnehmer konfigurieren . . . 751
15.4.2 Leitungstrennung für einen Notruf . . . 751
15.4.2.1 Wie Sie die Leitungstrennung für einen Notruf aktivieren oder deaktivieren . . . 752
15.4.3 Nur für USA, Kanada: Notrufdienst E911 . . . 752
15.4.3.1 Wie Sie CLIP / LIN bearbeiten . . . 753
15.4.4 Notrufe in Kombination mit Mobile Logon . . . 753
15.4.4.1 Konfiguration des Notrufszenarios . . . 754
15.5 Anrufsteuerungsdienst (Call Admission Control) . . . 756
15.5.1 Einschränkung der Anzahl gleichzeitiger Gespräche über ITSP . . . 757
15.5.2 Einschränkung des Bandbreitenbedarfs bei Gateway-Gesprächen . . . 757
15.5.3 Einschränkung der Anzahl der Gespräche in Vernetzungszenarien . . . 757
15.6 Gemeinschaftsanlage . . . 758
15.6.1 Kurzwahl zentral in Gemeinschaftsanlagen . . . 759

16 Attendants . . . 760
16.1 AutoAttendant . . . 760
16.1.1 Company AutoAttendant (UC Smart) . . . 762
16.1.1.1 Wie Sie einen eingerichteten Company AutoAttendant konfigurieren . . . 763
16.1.1.2 Wie Sie einen neuen Company AutoAttendant einrichten . . . 764
16.1.2 Company AutoAttendant (UC Suite) . . . 766
16.1.2.1 Zeitpläne . . . 767

16.1.2.2 Templates . . . 773
16.1.3 Xpressions Compact . . . 778
16.2 OpenStage Attendant . . . 778
16.3 OpenScape Business Attendant . . . 779
16.3.1 OpenScape Business BLF . . . 782
16.3.2 BLF-Server . . . 783
16.3.3 Einrichtebeispiele für OpenScape Business Attendant, OpenScape Business BLF und BLF-Server 783
16.3.3.1 Szenario 1: OpenScape Business Attendant an einem OpenScape Business Einzelsystem . . 783
16.3.3.2 Szenario 2: Zwei oder mehrere OpenScape Business Attendant an einem OpenScape Business Einzelsystem . . . 790
16.3.3.3 Szenario 3: OpenScape Business Vernetzung mit jeweils eigenen OpenScape Business Attendants (netzweite BLF und Anwesenheitsstatus über BLF-Server) . . . 791
16.3.3.4 Szenario 4: OpenScape Business Vernetzung mit zentralem OpenScape Business Attendant (netzweite BLF und Anwesenheitsstatus über BLF-Server) . . . 792
16.3.3.5 Szenario 5: OpenScape Business BLF an einem OpenScape Business Einzelsystem . . . 794
16.3.3.6 Szenario 6: OpenScape Business BLF an einem OpenScape Business Netzverbund (BLF und Anwesenheitsstatus über BLF-Server) . . . 796
16.3.3.7 Szenario 7: BLF-Server einrichten . . . 797
16.4 myAttendant . . . 799
16.4.1 Teilnehmerverwaltung . . . 800
16.4.2 Nachrichten-Center . . . 801
16.4.3 Szenario 1: Wie Sie myAttendant an einem OpenScape Business Einzelsystem einrichten . . . 802
16.4.4 Szenario 2: Wie Sie zwei oder mehrere myAttendant an einem OpenScape Business Einzelsystem einrichten . . . 802
16.4.5 Szenario 3: Wie Sie eine OpenScape Business Vernetzung mit zentralem myAttendant einrichten 804
16.5 Abwurfplatz . . . 805
16.5.1 Wie Sie Abwurfplatz und Abwurfkriterien konfigurieren . . . 807
16.5.2 Wie Sie einen zentralen Abwurfplatz konfigurieren . . . 807
16.5.3 Wie Sie Abwurf bei Codeschloss konfigurieren . . . 808
16.5.4 Wie Sie Abwurf bei Ansage konfigurieren . . . 808

17 Multimedia Contact Center . . . 809
17.1 Contact Center Clients . . . 809
17.1.1 myAgent . . . 810
17.1.2 Voraussetzungen für myAgent . . . 811
17.1.3 myReports . . . 813
17.1.3.1 Wie Sie myReports-Administrator-Kennwort zurücksetzen . . . 815
17.1.4 Voraussetzungen für myReports . . . 816
17.1.5 Hinweise zur gleichzeitigen Nutzung von myAgent und UC Suite Clients . . . 818
17.2 Agenten . . . 819
17.2.1 Berechtigungsabhängige Funktionen für Agenten . . . 819
17.2.2 Bevorzugte Agenten . . . 820
17.2.3 Agent in mehreren Warteschlangen . . . 821
17.2.4 Contact Center-Pausen . . . 821
17.3 Warteschlangen und Zeitpläne . . . 821
17.3.1 Warteschlangen . . . 821
17.3.2 Zeitpläne . . . 823
17.3.3 Nachbearbeitung . . . 830
17.3.4 Servicegrad . . . 831
17.3.5 Wandanzeige (Wallboard) . . . 831
17.3.6 Agentenrückruf . . . 831
17.4 VIP-Betreuung . . . 832

17.4.1 VIP-Anruferpriorität . . . 832
17.4.2 VIP-Rufliste . . . 832
17.5 Rückfalllösung (Fallback-Lösung) . . . 833
17.6 Konfiguration des Contact Centers . . . 835
17.6.1 Beispiel für eine Contact-Center-Konfiguration . . . 836
17.6.1.1 Wie Sie UCD-Gruppen für das Beispiel-Contact-Center konfigurieren . . . 838
17.6.1.2 Wie Sie eine Rückfalllösung (Fallback-Lösung) für das Beispiel-Contact-Center konfigurieren 839
17.6.1.3 Wie Sie einen Teilnehmer als Agent für das Beispiel-Contact-Center konfigurieren . . . 840
17.6.1.4 Wie Sie Ansagen für das Beispiel-Contact-Center aufnehmen . . . 841
17.6.1.5 Wie Sie Ansagen für das Beispiel-Contact-Center laden . . . 842
17.6.1.6 Wie Sie den Zeitplan Standard Schedule XYZ für das Beispiel-Contact-Center hinzufügen . . 842
17.6.1.7 Wie Sie den Zeitplan Standard Schedule Hotline für das Beispiel-Contact-Center hinzufügen 847
17.6.1.8 Wie Sie Warteschlangen für das Beispiel-Contact-Center hinzufügen . . . 849
17.6.1.9 Wie Sie Agenten den Warteschlangen des Beispiel-Contact-Centers zuordnen . . . 851
17.6.2 Vorgehensweise bei der Konfiguration . . . 853
17.6.2.1 Wie Sie UCD-Gruppen für das Contact Center konfigurieren . . . 853
17.6.2.2 Wie Sie einen Teilnehmer als Agent konfigurieren . . . 854
17.6.2.3 Wie Sie eine individuelle Ansage für das Contact Center aufnehmen . . . 855
17.6.2.4 Wie Sie eine individuelle Ansage für das Contact Center laden . . . 856
17.6.2.5 Wie Sie einen Zeitplan hinzufügen . . . 856
17.6.2.6 Wie Sie einen Zeitplan ändern . . . 860
17.6.2.7 Wie Sie einen Zeitplan löschen . . . 861
17.6.2.8 Wie Sie eine Regel (CCV) als PDF-Datei speichern . . . 862
17.6.2.9 Wie Sie eine Warteschlange hinzufügen . . . 863
17.6.2.10 Wie Sie eine Warteschlange ändern . . . 866
17.6.2.11 Wie Sie eine Warteschlange aktivieren oder deaktivieren . . . 869
17.6.2.12 Wie Sie einen Pilot für eingehende Faxnachrichten in Warteschlangen konfigurieren . . . 870
17.6.2.13 Wie Sie Sollwerte für Servicegrad festlegen . . . 870
17.6.2.14 Wie Sie die VIP-Anruferpriorität festlegen . . . 871
17.6.2.15 Wie Sie eine VIP-Rufliste bearbeiten . . . 872
17.6.2.16 Wie Sie einen bevorzugten Agenten festlegen . . . 873
17.6.2.17 Wie Sie einen bevorzugten Agenten löschen . . . 873
17.6.2.18 Wie Sie eine Contact Center-Pause hinzufügen . . . 874
17.6.2.19 Wie Sie eine Contact Center-Pause ändern . . . 874
17.6.2.20 Wie Sie eine Contact Center-Pause löschen . . . 875
17.6.2.21 Wie Sie den Nachbearbeitungsgrund für "Einfache Nachbearbeitung" hinzufügen . . . 875
17.6.2.22 Wie Sie den Nachbearbeitungsgrund für "Einfache Nachbearbeitung" ändern . . . 876
17.6.2.23 Wie Sie den Nachbearbeitungsgrund für "Einfache Nachbearbeitung" löschen . . . 876
17.6.2.24 Wie Sie den Nachbearbeitungsgrund für "Mehrfache Nachbearbeitung" hinzufügen . . . 877
17.6.2.25 Wie Sie den Nachbearbeitungsgrund für "Mehrfache Nachbearbeitung" ändern . . . 878
17.6.2.26 Wie Sie den Nachbearbeitungsgrund für "Mehrfache Nachbearbeitung" löschen . . . 878
17.6.2.27 Wie Sie einen Agent einer Warteschlange zuordnen . . . 879
17.6.2.28 Wie Sie einen Agent aus einer Warteschlange entfernen . . . 880
17.7 Hinweise zum Einsatz des Contact Centers . . . 881
17.7.1 Einschränkungen beim Betrieb des Contact Centers . . . 881
17.8 Hinweise zum Einsatz von DECT-Telefonen . . . 883
17.9 Berichte . . . 884
17.9.1 Vordefinierte Berichtsvorlagen . . . 886
17.9.2 Berichts-Designer . . . 886

18 Mobility . . . 887
18.1 Integrierte Mobilitätslösungen . . . 887

18.2 Mobilität unterwegs 887
18.2.1 myPortal for Mobile 888
18.2.1.1 Voraussetzungen für myPortal for Mobile 889
18.2.2 myPortal to go 890
18.2.2.1 Voraussetzungen für myPortal to go 892
18.2.3 Mobility Entry 893
18.2.4 Vergleich Mobile Clients und Mobility Entry 894
18.2.5 Abhängigkeiten für Mobile Clients und Mobility Entry 896
18.2.6 One Number Service 898
18.2.7 Dual-Mode-Telefonie 898
18.2.8 Konfiguration von myPortal for Mobile und Mobility Entry 899
18.2.8.1 Wie Sie ein GSM-Mobiltelefon integrieren 900
18.2.8.2 Wie Sie ein Dual-Mode-Telefon (GSM/WLAN) mit SIP-Client integrieren 901
18.2.8.3 Wie Sie die Web-Schnittstelle für Mobiltelefone und Web-Clients aktivieren 903
18.2.8.4 Wie Sie die Mobiltelefon-Integration löschen 904
18.3 Mobilität im Büro 904
18.3.1 DeskSharing 904
18.3.2 Integrierte Cordless-Lösung 905
18.3.2.1 Cordless-Direktanschaltung (DECT Light) 907
18.3.2.2 Cordless-Baugruppenanschaltung 907
18.3.2.3 Systemausbau 908
18.3.2.4 Cordless/DECT-Telefone 908
18.3.3 Konfiguration der integrierten Cordless-Lösung 909
18.3.3.1 Wie Sie die DECT-Systemkennung eingeben und weitere Cordless-Parameter (systemweite Daten) konfigurieren 910
18.3.3.2 Wie Sie Cordless-Basisstationen konfigurieren 910
18.3.3.3 Wie Sie DECT-Telefone erstmalig konfigurieren 911
18.3.3.4 Wie Sie ein DECT-Telefon (OpenStage/Gigaset-Mobilteil) an Cordless anmelden 911
18.3.3.5 Wie Sie weitere DECT-Telefone hinzufügen 912
18.3.3.6 Wie Sie DECT-Telefone löschen 913
18.3.3.7 Wie Sie die Multi-SLC-Parameter konfigurieren 913
18.3.3.8 Wie Sie die Daten zu den Basisstationen abfragen 914
18.3.3.9 Wie Sie den Hinweiston der Message Waiting Indication (MWI) für DECT-Telefone aktivieren 914
18.3.3.10 Wie Sie den Anmeldestatus der DECT-Telefone abfragen 915
18.3.4 Cordless IP 915
18.3.5 WLAN-Telefone und Access Points 916
18.3.5.1 Anforderungen an das WLAN 916
18.4 Mobilität zu Hause 916
18.4.1 Konfiguration für VPN 917
18.4.2 Konfiguration für SIP@Home 918
18.4.2.1 Wie Sie SIP@Home für SIP-Teilnehmer aktivieren oder deaktivieren 919
18.4.2.2 Wie Sie einen STUN-Server für SIP@Home angeben 920

19 Security 921
19.1 Firewall 921
19.1.1 Porthandling 921
19.1.1.1 Portfreigabe 922
19.1.1.2 Wie Sie die Portfreigabe konfigurieren 923
19.1.1.3 Port-Verwaltung 923
19.1.1.4 Wie Sie globale Port-Manager-Einstellungen ändern 924
19.1.2 NAT 924

19.1.2.1 Wie Sie eine NAT-Regel konfigurieren . . . 925
19.1.2.2 Wie Sie mehrere NAT-Regeln mit dem NAT-Tabelleneditor konfigurieren . . . 926
19.1.2.3 Wie Sie eine NAT-Regel löschen . . . 927
19.1.3 Application Firewall . . . 927
19.1.3.1 Wie Sie die Konfiguration der Application Firewall anzeigen . . . 928
19.1.3.2 Wie Sie Dienste über die Application Firewall einschränken . . . 928
19.1.3.3 Wie Sie die Konfiguration der Application Firewall löschen . . . 929
19.1.4 Diensteverwaltung (OpenScape Business S) . . . 929
19.1.4.1 Wie Sie Dienste hinzufügen oder sperren . . . 930
19.2 Signaling and Payload Encryption SPE . . . 930
19.2.1 Wie Sie SPE Unterstützung aktivieren oder deaktivieren . . . 933
19.2.2 Wie Sie SPE-Sicherheitseinstellungen ändern . . . 933
19.2.3 Wie Sie ein SPE-Zertifikat und den privaten Schlüssel importieren (PKCS#12) . . . 934
19.2.4 Wie Sie das SPE CA-Zertifikat importieren . . . 934
19.2.5 Wie Sie SPE für einen Teilnehmer aktivieren oder deaktivieren . . . 935
19.3 Virtual Private Network VPN . . . 935
19.3.1 Anforderungen für VPN . . . 936
19.3.2 Anbindung von Teleworkern über VPN . . . 938
19.3.2.1 Wie Sie die Anbindung von Teleworkern über VPN konfigurieren . . . 940
19.3.2.2 Wie Sie die Teleworker-Daten exportieren . . . 942
19.3.3 Vernetzung von Kommunikationssystemen über VPN . . . 942
19.3.3.1 Wie Sie die Vernetzung über VPN konfigurieren . . . 943
19.3.3.2 Wie Sie Topologie-Daten einer VPN-Vernetzung exportieren und importieren . . . 946
19.3.4 VPN - Sicherheitsmechanismen . . . 946
19.3.5 VPN - Zertifikate . . . 948
19.3.5.1 VPN - Wie Sie Lightweight-CA-Zertifikate generieren . . . 950
19.3.5.2 VPN - Zertifikatsverwaltung - Wie Sie ein Zertifikat anzeigen . . . 951
19.3.5.3 VPN - Wie Sie ein Trusted CA-Zertifikat importieren (X.509) . . . 952
19.3.5.4 VPN - Peer Zertifikate - Wie Sie eine Zertifikatsanforderung (CSR) generieren . . . 952
19.3.5.5 VPN - Peer Zertifikate - Wie Sie ein Zertifikat (PKCS#12) generieren . . . 953
19.3.5.6 VPN - Wie Sie ein Peer Zertifikat importieren (PKCS#12) . . . 954
19.3.6 VPN-Clients . . . 954
19.3.6.1 NCP VPN Client Einstellungen . . . 955
19.3.6.2 Wie Sie einen NCP VPN Client konfigurieren . . . 958
19.3.6.3 Wie Sie einen Shrew Soft VPN Client konfigurieren . . . 958
19.3.6.4 Wie Sie einen iOS VPN Client konfigurieren . . . 959
19.3.6.5 Wie Sie einen Mac OS-X VPN Client konfigurieren . . . 960
19.3.7 VPN - Dienste . . . 960
19.3.7.1 VPN - Aktive Dienste - Wie Sie alle IPsec-Dienste anzeigen . . . 961
19.3.7.2 VPN - Aktive Dienste - Wie Sie einen speziellen IPsec-Dienst anzeigen . . . 961
19.3.7.3 VPN - Konfigurierte Dienste - Wie Sie alle IPsec-Dienste anzeigen . . . 961
19.3.7.4 VPN - Konfigurierte Dienste - Wie Sie den IPsec-Dienst ändern . . . 962
19.3.7.5 VPN - Konfigurierte Dienste - Wie Sie den IPsec-Dienst umbenennen . . . 962
19.3.7.6 VPN - Konfigurierte Dienste - Wie Sie den IPsec-Dienst löschen . . . 963
19.3.8 VPN - Tunnel . . . 963
19.3.8.1 VPN - Aktive Tunnel - Wie Sie allgemeine Tunneldaten anzeigen . . . 963
19.3.8.2 VPN - Aktive Tunnel - Wie Sie Regeln für alle Tunnel anzeigen . . . 964
19.3.8.3 VPN - Konfigurierte Tunnel - Wie Sie allgemeine Tunneldaten anzeigen . . . 964
19.3.8.4 VPN - Konfigurierte Tunnel - Wie Sie Regeln für alle Tunnel anzeigen . . . 965
19.3.8.5 VPN - Wie Sie einen konfigurierten Tunnel hinzufügen . . . 965
19.3.9 VPN - Regeln . . . 967

19.3.9.1 VPN - Aktive Regeln - Wie Sie Regeln anzeigen 968
19.3.9.2 VPN - Aktive Regeln - Wie Sie spezielle Regel anzeigen 968
19.3.9.3 VPN - Konfigurierte Regeln - Wie Sie alle Regeln anzeigen 969
19.3.9.4 VPN - Konfigurierte Regeln - Wie Sie eine Regel hinzufügen 969
19.3.9.5 VPN - Wie Sie eine Regel ändern 970
19.3.9.6 VPN - Wie Sie eine Regel für die Gegenrichtung hinzufügen 971
19.3.9.7 VPN - Wie Sie eine Regel löschen 971
19.3.10 PKI-Server 972
19.3.10.1 VPN - Wie Sie den PKI-Server anzeigen 972
19.3.10.2 VPN - Wie Sie einen PKI-Server hinzufügen 972
19.4 Zertifikatshandling 973
19.4.1 Wie Sie ein CA-Zertifikat generieren 974
19.4.2 Wie Sie ein selbstsigniertes Zertifikat generieren 974
19.4.3 Wie Sie eine Zertifikatsanforderung (CSR) generieren 975
19.4.4 Wie Sie ein Server-Zertifikat importieren (PKCS#12) 975
19.4.5 Wie Sie Zertifikate anzeigen 976
19.4.6 Wie Sie ein Zertifikat löschen 976
19.4.7 Wie Sie ein Zertifikat exportieren (X.509) 977
19.4.8 Wie Sie ein verlängertes Zertifikat importieren (X.509) 977
19.4.9 Wie Sie ein Zertifikat aktivieren 978
19.5 Web-Sicherheit 978
19.5.1 Verbindungen zum Web-Server 978
19.5.1.1 Wie Sie die Verbindungen zum Web-Server konfigurieren (UC Suite) 979
19.5.1.2 Wie Sie die Verbindungen zum Web-Server konfigurieren (UC Smart) 979
19.5.2 Admin-Protokoll 980
19.5.2.1 Wie Sie das Admin.-Protokoll laden 980
19.5.2.2 Wie Sie die Admin.-Protokoll-Sprache ändern 980
19.6 Schutz vor SIP-Attacken (SIP Attack Protection) 981

20 Vernetzung von OpenScape Business 982
20.1 Vernetzungsplan 983
20.1.1 Homogene und inhomogene Netze 983
20.1.1.1 Wie Sie die Übersicht aller OpenScape Business Knoten anzeigen 984
20.1.1.2 Wie Sie die Teilnehmer aller OpenScape Business Knoten anzeigen 984
20.1.1.3 Wie Sie Teilnehmer über alle OpenScape Business Knoten suchen 984
20.1.2 Single- und Multi-Gateway 985
20.2 Netzweite Leistungsmerkmale 986
20.2.1 Netzweite Leistungsmerkmale der UC Suite 986
20.2.2 Netzweite Voice-Leistungsmerkmale 991
20.3 Lizenzierung eines Netzverbundes 992
20.4 Anforderungen an die Vernetzung 992
20.4.1 Anforderungen an die LAN-Vernetzung 993
20.4.2 Anforderungen an die WAN-Vernetzung 995
20.4.3 Rufnummernplan im Netz 997
20.4.3.1 Wahl von öffentlichen Rufnummern im Netz 998
20.5 Wegeoptimierung (Path Replacement) 998
20.5.1 Wie Sie die Wegeoptimierung (Path Replacement) aktivieren oder deaktivieren 999
20.6 Vernetzungsszenarien 999
20.6.1 Abhängigkeiten und Einschränkungen 1000
20.6.2 Szenario 1: Vernetzung von mehreren OpenScape Business X 1001
20.6.3 Szenario 1: Netzweite Leistungsmerkmale 1002
20.6.4 Szenario 1: Konfiguration 1006

20.6.4.1 Wie Sie die Basisinstallation für Knoten 1 (Master) konfigurieren. 1008
20.6.4.2 Wie Sie die Vernetzung für Knoten 1 (Master) konfigurieren 1009
20.6.4.3 Wie Sie die Basisinstallation für Knoten 2 (Slave) konfigurieren. 1010
20.6.4.4 Wie Sie die Vernetzung für Knoten 2 (Slave) konfigurieren 1011
20.6.4.5 Wie Sie die Vernetzungsfunktion für den Master kontrollieren 1012
20.6.4.6 Wie Sie Richtungen und Richtungsparameter konfigurieren (ISDN-Amt für den Master). . . . 1012
20.6.4.7 Wie Sie Richtungen und Richtungsparameter (Rtg. 16) konfigurieren (Master) 1013
20.6.4.8 Wie Sie LCR für die Vernetzung konfigurieren (Master) 1014
20.6.4.9 Wie Sie die Richtung und Richtungsparameter konfigurieren (Slave) 1015
20.6.4.10 Wie Sie LCR für die Vernetzung konfigurieren (Slave) 1015
20.6.5 Szenario 2: Vernetzung von OpenScape Business X mit OpenScape Business S (Single Gateway) 1017
20.6.6 Szenario 2: Netzweite Leistungsmerkmale. 1018
20.6.7 Szenario 2: Konfiguration 1022
20.6.7.1 Wie Sie die Basisinstallation für Knoten 1 (Master) konfigurieren. 1026
20.6.7.2 Wie Sie die Vernetzung für Knoten 1 (Master) konfigurieren 1027
20.6.7.3 Wie Sie die Basisinstallation für Knoten 2 (Slave) konfigurieren. 1028
20.6.7.4 Wie Sie die Vernetzung für Knoten 2 (Slave) konfigurieren 1029
20.6.7.5 Wie Sie die Basisinstallation für Knoten 3 (Slave) konfigurieren. 1030
20.6.7.6 Vernetzung konfigurieren für Knoten 3 (Slave) 1031
20.6.7.7 Wie Sie die Vernetzungsfunktion für den Master kontrollieren 1032
20.6.7.8 Wie Sie LCR für die Vernetzung konfigurieren (Knoten 3, Slave). 1032
20.6.7.9 Wie Sie LCR für die Vernetzung konfigurieren (Knoten 2) 1034
20.6.7.10 Wie Sie Richtungen und Richtungsparameter konfigurieren (Knoten 1, Master) 1036
20.6.7.11 Wie Sie Richtungen und Richtungsparameter (Rtg. 16) konfigurieren (Knoten 1) 1037
20.6.7.12 Wie Sie LCR für die Vernetzung konfigurieren (Knoten 1) 1037
20.6.8 Szenario 3: Vernetzung von Open Scape Business X und OpenScape Business S (Multi Gateway). 1039
20.6.9 Szenario 3: Netzweite Leistungsmerkmale. 1041
20.6.10 Szenario 3: Konfiguration 1045
20.6.10.1 Wie Sie die Basisinstallation für Knoten 4 (OpenScape Business S, Master) konfigurieren. 1051
20.6.10.2 Wie Sie die Vernetzung für Knoten 4 (Master) konfigurieren 1052
20.6.10.3 Wie Sie die Basisinstallation für Knoten 1 (Slave) konfigurieren. 1053
20.6.10.4 Wie Sie die Vernetzung für Knoten 1 (Slave) konfigurieren 1054
20.6.10.5 Wie Sie die Basisinstallation für Knoten 2 (Slave) konfigurieren. 1054
20.6.10.6 Wie Sie die Vernetzung für Knoten 2 (Slave) konfigurieren 1055
20.6.10.7 Wie Sie die Basisinstallation für Knoten 3 (Slave) konfigurieren. 1056
20.6.10.8 Wie Sie die Vernetzung für Knoten 3 (Slave) konfigurieren 1057
20.6.10.9 Wie Sie die Vernetzungsfunktion für den Master kontrollieren 1058
20.6.10.10 Wie Sie ein Multi-Gateway für Knoten 4 (Master) konfigurieren 1058
20.6.10.11 Wie Sie die Richtung und Richtungsparameter konfigurieren (Knoten 1, Slave) 1059
20.6.10.12 Wie Sie LCR für die Vernetzung konfigurieren (Knoten 1, Slave). 1060
20.6.10.13 Wie Sie die Richtung und Richtungsparameter konfigurieren (Knoten 2, Slave) 1062
20.6.10.14 Wie Sie LCR für die Vernetzung konfigurieren (Knoten 2, Slave). 1063
20.6.10.15 Wie Sie die Richtung und Richtungsparameter konfigurieren (Knoten 3, Slave) 1065
20.6.10.16 Wie Sie LCR für die Vernetzung konfigurieren (Knoten 3, Slave). 1066
20.6.10.17 Wie Sie die Richtung und Richtungsparameter konfigurieren (Knoten 4, Master) 1068
20.6.10.18 Wie Sie LCR für die Vernetzung konfigurieren (Knoten 4, Master). 1069
20.6.11 Szenario 4: Vernetzung von OpenScape Business X und OpenScape 4000/HiPath 4000 1072
20.6.12 Szenario 4: Netzweite Leistungsmerkmale. 1075
20.6.13 Szenario 5: Vernetzung von OpenScape Business X und OpenScape Voice 1080
20.6.14 Szenario 5: Netzweite Leistungsmerkmale. 1081

20.6.15 Szenario 6: Anbindung von externen Anschaltungen an OpenScape Business über SIP-Interconnection 1084
20.6.16 Szenario 7: Offene Nummerierung in OpenScape Business X Netzwerken 1086
20.6.17 Szenario 7: Konfiguration. 1087
20.6.18 Szenario 8: Vernetzung über ISDN 1088
20.6.19 Szenario 9: OpenScape Business Netzverbund mit zentralem ITSP-Amtsanschluss. 1090
20.7 Zentraler Abwurfplatz im Netzverbund (nicht für USA) 1092
20.7.1 Wie Sie den zentralen Abwurfplatz im Multi-Gateway-Netzverbund konfigurieren 1093
20.8 Presence Manager 1095
20.9 Synchronisationsstatus im Netzverbund 1095
20.9.1 Manuelle Synchronisierung im Netzverbund 1096
20.9.2 Wie Sie eine Synchronisierung manuell starten 1097
20.10 Survivability 1097
20.10.1 Wie Sie Survivability konfigurieren. 1099
20.11 Entfernung eines Knotens aus dem Netzverbund. 1099

21 Anschaltungen 1101
21.1 Analoges Ansagegerät 1101
21.1.1 Wie Sie ein analoges Ansagegerät hinzufügen 1102
21.1.2 Wie Sie die Ansageverzögerung ändern 1103
21.2 Türsprechstelle und Türöffner 1103
21.2.1 DoorLine a/b T01-T04 1103
21.2.1.1 Wie Sie den Teilnehmerport der Doorline a/b T01-T04 konfigurieren 1104
21.2.1.2 Wie Sie die Nebenstelle für die Doorline a/b T01-T04 konfigurieren 1105
21.2.2 DoorCom Analog 1105
21.2.2.1 Wie Sie den Teilnehmerport der DoorCom Analog konfigurieren 1106
21.2.2.2 Wie Sie die Nebenstelle für die DoorCom Analog konfigurieren 1106
21.2.3 Türfreisprecheinrichtung mit Verstärker (TFE-S) 1107
21.2.3.1 Wie Sie die Türsprechstelle konfigurieren 1108
21.2.4 Lautsprecher 1109
21.2.4.1 Wie Sie die analoge Teilnehmer-Schnittstelle für einen Lautsprecher konfigurieren 1110
21.2.4.2 Wie Sie die analoge Teilnehmer-Schnittstelle für den Anschluss eines Verstärker am TFE S Modul konfigurieren 1110
21.3 Aktoren 1111
21.3.1 Wie Sie einen Aktor konfigurieren 1113
21.4 Sensoren. 1113
21.5 OpenStage Gate View 1115
21.5.1 Rechtliche Rahmenbedingungen. 1115
21.5.2 Komponenten. 1116
21.5.3 Funktionsübersicht. 1116
21.5.4 Menü 1117
21.5.5 OpenStage Gate View Ersteinrichtung 1118
21.5.5.1 Wie Sie die Server-Software erstmals starten 1119
21.5.5.2 Wie Sie Ihr Administrator-Passwort ändern 1119
21.5.5.3 Wie Sie eine Kamera hinzufügen 1120
21.5.5.4 Wie Sie ein Telefon hinzufügen 1121
21.5.6 OpenStage Gate View Videoaufzeichnung 1121
21.5.6.1 Wie Sie die Videofunktion am Telefon einrichten 1122
21.5.6.2 Wie Sie vorhandene Aufzeichnungen bearbeiten 1123
21.5.7 OpenStage Gate View Türsprechstelle 1124
21.5.7.1 Wie Sie die Türsprechstelle einrichten 1124
21.5.8 OpenStage Gate View Benutzerverwaltung 1125

21.5.8.1 Wie Sie einen Benutzer hinzufügen . . . 1125
21.5.8.2 Wie Sie Benutzerdaten ändern . . . 1126
21.5.8.3 Wie Sie einen Benutzer löschen . . . 1126
21.5.9 OpenStage Gate View Server-Administration . . . 1127
21.5.9.1 Wie Sie die Administrationsoberfläche öffnen . . . 1127
21.5.9.2 Wie Sie Software-Informationen anzeigen . . . 1127
21.5.9.3 Wie Sie Serverdaten löschen . . . 1127
21.5.9.4 Wie Sie die Protokolldatei anzeigen und abspeichern . . . 1128
21.5.10 OpenStage Gate View Anpassungen . . . 1128
21.5.10.1 Wie Sie eine Kamera manuell hinzufügen . . . 1129
21.5.10.2 Wie Sie eine Kamera löschen . . . 1130
21.5.10.3 Wie Sie ein Telefon manuell hinzufügen . . . 1130
21.5.10.4 Wie Sie ein Telefon löschen . . . 1131
21.5.10.5 Wie Sie den OpenStage Gate View Server deaktivieren . . . 1131

22 Application Connectivity . . . 1132
22.1 CSTA . . . 1132
22.1.1 Wie Sie die Portnummer für CSTA ändern . . . 1134
22.1.2 Wie Sie den CMD für die Nutzung von TAPI 120 aktivieren oder deaktivieren . . . 1135
22.1.3 Wie Sie den DSS-Server für die Nutzung von netzweiten DSS-Tasten aktivieren oder deaktivieren . . . 1135
22.1.4 Wie Sie den CSP aktivieren oder deaktivieren . . . 1136
22.1.5 Wie Sie Media Extension Bridge aktivieren oder deaktivieren . . . 1136
22.2 OpenScape Business TAPI 120/170 . . . 1137
22.2.1 OpenScape Business TAPI 120 . . . 1138
22.2.2 OpenScape Business TAPI 170 . . . 1143
22.3 Web Services Interface . . . 1148
22.4 Open Directory Service . . . 1149
22.4.1 Wie Sie Open Directory Service aktivieren oder deaktivieren . . . 1153
22.4.2 Wie Sie Open Directory Service neu starten . . . 1153
22.4.3 Wie Sie das Passwort für Zugriff auf Open Directory Service konfigurieren . . . 1154
22.4.4 Wie Sie eine externe Datenquelle für Open Directory Service hinzufügen . . . 1154
22.4.5 Wie Sie eine Vorschau auf LDAP-Suchergebnis für Open Directory Service durchführen . . . 1156
22.4.6 Wie Sie eine externe Datenquelle für Open Directory Service löschen . . . 1157
22.5 XMPP . . . 1157
22.5.1 Wie Sie XMPP konfigurieren . . . 1158
22.6 Application Launcher . . . 1159
22.6.1 Voraussetzungen für Application Launcher . . . 1159
22.6.2 Profil mit Konfigurationsdaten von Application Launcher . . . 1160
22.6.2.1 Wie Sie das Profil mit Konfigurationsdaten von Application Launcher bereitstellen . . . 1161

23 Accounting . . . 1162
23.1 Verbindungsdaten . . . 1162
23.1.1 Erfassung von Verbindungsdaten . . . 1162
23.1.1.1 Wie Sie die Erfassung von Verbindungsdaten aktivieren oder deaktivieren . . . 1163
23.1.1.2 Wie Sie die Protokollierung der Verbindungsdauer aktivieren oder deaktivieren . . . 1164
23.1.1.3 Wie Sie die Protokollierung von Geldbeträgen oder Tarifeinheiten konfigurieren . . . 1164
23.1.1.4 Wie Sie Tariffaktor, Währung und Rechengenauigkeit konfigurieren . . . 1164
23.1.1.5 Wie Sie die Protokollierung der letzten vier Ziffern aktivieren oder deaktivieren . . . 1165
23.1.1.6 Wie Sie die Protokollierung gehender Anrufe ohne Verbindung aktivieren oder deaktivieren 1166
23.1.1.7 Wie Sie die Protokollierung kommender Verbindungen aktivieren oder deaktivieren . . . 1166
23.1.1.8 Wie Sie das Verbindungsprotokoll aktivieren oder deaktivieren . . . 1167
23.1.1.9 Wie Sie die Protokollierung der MSN aktivieren oder deaktivieren . . . 1167

23.1.1.10 Wie Sie das Dezimalformat aktivieren oder deaktivieren . . . 1167
23.1.2 Projektkennzahlen . . . 1168
23.1.2.1 Wie Sie eine Projektkennzahl konfigurieren . . . 1169
23.1.2.2 Wie Sie ein PKZ-Prüfverfahren konfigurieren . . . 1170
23.1.2.3 Wie Sie Wahlwiederholung mit PKZ aktivieren oder deaktivieren . . . 1170
23.2 Anzeige und Übertragung von Verbindungsdaten . . . 1170
23.2.1 Übermittlung von Geldbeträgen (nicht für USA) . . . 1171
23.2.1.1 Wie Sie die Übermittlung von Geldbeträgen konfigurieren . . . 1171
23.2.2 Anzeige der Verbindungskosten am Telefon . . . 1172
23.2.3 Anzeige der Verbindungsdauer am Telefon . . . 1172
23.2.3.1 Wie Sie die Anzeige der Verbindungsdauer aktivieren oder deaktivieren . . . 1173
23.2.4 Übertragung von Verbindungsdaten . . . 1173
23.2.4.1 Wie Sie das Format auswählen . . . 1180
23.2.4.2 Wie Sie die Übertragung von Verbindungsdaten über HTTPS aktivieren oder deaktivieren . . . 1180
23.3 Kostenkontrolle . . . 1181
23.3.1 Hinweis auf teure Verbindungswege . . . 1181
23.3.1.1 Wie Sie einen Hinweis auf einen teuren Verbindungsweg konfigurieren . . . 1181
23.3.2 Schutz vor Gebührenbetrug . . . 1182
23.3.2.1 Wie Sie den Schutz vor Gebührenbetrug aktivieren oder deaktivieren . . . 1182
23.4 Accounting-Tools . . . 1182
23.4.1 Accounting Manager . . . 1183
23.4.2 Teledata Office . . . 1183

24 Maintenance . . . 1184
24.1 Telefonie-Konfiguration . . . 1184
24.1.1 Datum und Uhrzeit . . . 1184
24.1.1.1 Wie Sie Datum und Uhrzeit manuell konfigurieren . . . 1185
24.1.1.2 Wie Sie die Zeitzone einstellen . . . 1185
24.1.1.3 Wie Sie das Datumsformat konfigurieren . . . 1186
24.1.2 SNTP . . . 1186
24.1.2.1 Wie Sie Datum und Uhrzeit von einem SNTP-Server beziehen . . . 1187
24.1.3 Telefon-Logos . . . 1187
24.1.3.1 Wie Sie ein Telefon-Logo ins System laden . . . 1187
24.1.3.2 Wie Sie ein Telefon-Logo an Systemtelefone verteilen . . . 1188
24.1.3.3 Wie Sie ein Telefon-Logo löschen . . . 1188
24.1.4 Kundenindividuelle Displayanzeige . . . 1189
24.1.4.1 Wie Sie die kundenindividuelle Displayanzeige (System-Name) ändern . . . 1189
24.1.5 Mehrsprachige Textausgabe . . . 1190
24.1.6 Flexible Menüs . . . 1190
24.1.6.1 Wie Sie das flexible Menü ändern . . . 1190
24.1.7 Wartemusik . . . 1191
24.1.7.1 Wie Sie interne Wartemusik importieren . . . 1192
24.1.7.2 Wie Sie die Funktion der internen Wartemusik konfigurieren . . . 1193
24.1.8 Ansagen . . . 1193
24.1.8.1 Wie Sie Ansagen konfigurieren (UC Smart) . . . 1194
24.1.8.2 Wie Sie Ansagen konfigurieren (UC Suite) . . . 1194
24.1.8.3 Wie Sie den Announcement Player konfigurieren (nur mit UC Booster) . . . 1195
24.1.9 Teilnehmer-zu-Teilnehmer Zeichengabe . . . 1200
24.1.10 Sprachkanal-Signalisierungsschutz . . . 1200
24.1.11 Zeitparameter . . . 1200
24.1.12 Steuerung von Centrex-Leistungsmerkmalen . . . 1200
24.1.12.1 Wie Sie die Steuerung von Centrex-Leistungsmerkmalen aktivieren oder deaktivieren . . . 1201
24.2 Sichern und Wiederherstellen . . . 1201

24.2.1 Backup-Sets . . . 1202
24.2.1.1 Wie Sie sich Backup-Sets anzeigen lassen . . . 1203
24.2.1.2 Wie Sie Backup-Sets löschen . . . 1203
24.2.2 Backup-Medien . . . 1204
24.2.2.1 Wie Sie ein Backup-Medium hinzufügen . . . 1205
24.2.2.2 Wie Sie ein Backup-Medium bearbeiten . . . 1206
24.2.2.3 Wie Sie ein Backup-Medium löschen . . . 1206
24.2.3 Sofortiges Sichern . . . 1207
24.2.3.1 Wie Sie ein Backup-Set sofort sichern . . . 1207
24.2.4 Zeitgesteuertes Sichern . . . 1208
24.2.4.1 Wie Sie ein Backup-Set zeitgesteuert sichern . . . 1209
24.2.5 Wiederherstellen . . . 1209
24.2.5.1 Wie Sie ein Backup-Set wiederherstellen . . . 1210
24.3 Update . . . 1210
24.3.1 Nutzung eines lokalen Webservers . . . 1212
24.3.1.1 Wie Sie den Zugang zum lokalen Web-Server konfigurieren . . . 1213
24.3.2 Update des Kommunikationssystems . . . 1214
24.3.2.1 Wie Sie das System über einen Webserver aktualisieren . . . 1215
24.3.2.2 Wie Sie das System über ein USB-Medium aktualisieren . . . 1217
24.3.2.3 Wie Sie das System über einen Datei-Upload aktualisieren . . . 1218
24.3.2.4 Wie Sie das System über ein USB-Medium ohne WBM-Zugriff aktualisieren . . . 1219
24.3.3 Update der Systemtelefone . . . 1220
24.3.3.1 Wie Sie die Telefonsoftware ins System laden . . . 1220
24.3.3.2 Wie Sie die Telefonsoftware an Systemtelefone verteilen . . . 1221
24.3.3.3 Wie Sie die Telefonsoftware löschen . . . 1222
24.3.3.4 Wie Sie die automatische Verteilung der Telefonsoftware aktivieren oder deaktivieren . . . 1222
24.3.3.5 Wie Sie ein optiPoint WL2 professional von HFA auf SIP umrüsten . . . 1223
24.3.4 Software-Status . . . 1224
24.3.4.1 Wie Sie den Software-Status abfragen . . . 1224
24.4 Restart, Reload, Shutdown . . . 1224
24.4.1 Restart (Neustart) von OpenScape Business . . . 1225
24.4.1.1 Wie Sie einen Restart (Neustart) von OpenScape Business auslösen . . . 1226
24.4.2 Reload von OpenScape Business . . . 1226
24.4.2.1 Wie Sie einen Reload von OpenScape Business auslösen . . . 1227
24.4.3 Shutdown (Herunterfahren) von OpenScape Business X . . . 1228
24.4.3.1 Wie Sie OpenScape Business X herunterfahren . . . 1228
24.4.4 PIN für das kontrollierte Herunterfahren (Shutdown) von OpenScape Business X . . . 1228
24.4.4.1 Wie Sie eine PIN für das kontrollierte Herunterfahren (Shutdown) von OpenScape Business X konfigurieren . . . 1229
24.4.5 Restart (Neustart) der UC Booster Card (Application Board OCAB) . . . 1229
24.4.5.1 Wie Sie einen Restart (Neustart) der UC Booster Card (Application Board OCAB) auslösen 1230
24.4.6 Reload der UC Booster Card (Application Board OCAB) . . . 1230
24.4.6.1 Wie Sie einen Reload der UC Booster Card (Application Board OCAB) auslösen . . . 1231
24.4.7 Restart (Neustart) der UC Applikation . . . 1231
24.4.7.1 Wie Sie einen Restart (Neustart) der UC Applikation auslösen . . . 1231
24.4.8 Restart (Neustart) der Web Services . . . 1232
24.4.8.1 Wie Sie einen Restart (Neustart) der Web Services auslösen . . . 1232
24.5 Inventory-Management . . . 1233
24.5.1 Systemstatus . . . 1233
24.5.1.1 Wie Sie den Teilnehmer-Status abfragen . . . 1234
24.5.1.2 Wie Sie den Verbindungsaufbau-Status abfragen . . . 1235
24.5.1.3 Wie Sie den ITSP-Status abfragen . . . 1236

24.5.1.4 Wie Sie den VPN-Status abfragen 1237
24.5.1.5 Wie Sie IP-Adressen anzeigen 1238
24.5.2 Inventory 1239
24.5.2.1 Wie Sie das Inventory von OpenScape Business X abfragen 1240
24.5.2.2 Wie Sie das Inventory von OpenScape Business S abfragen 1241
24.6 Automatische Aktionen 1242
24.6.1 Automatische Aktion Garbage Collection 1242
24.6.1.1 Wie Sie die automatische Aktion Garbage Collection ändern 1242
24.6.1.2 Wie Sie die automatische Aktion Garbage Collection starten (aktivieren) 1243
24.6.1.3 Wie Sie die automatische Aktion Garbage Collection stoppen (deaktivieren) 1244
24.6.2 Automatische Aktion DLS Notification 1244
24.6.2.1 Wie Sie die automatische Aktion DLS Notification ändern 1245
24.6.2.2 Wie Sie die automatische Aktion DLS Notification starten (aktivieren) 1246
24.6.2.3 Wie Sie die automatische Aktion DLS Notification stoppen (deaktivieren) 1246
24.7 Power-Management 1246
24.7.1 Wie Sie das Power-Management aktivieren oder deaktivieren 1247
24.7.2 Wie Sie den Ethernet-Link-Modus der LAN-Schnittstellen ändern 1248
24.8 Überwachung und Wartung von OpenScape Business 1249
24.8.1 Prüfen einer Netzwerkverbindung von OpenScape Business X 1249
24.8.1.1 Wie Sie Ping senden 1249
24.8.1.2 Wie Sie Traceroute testen 1250
24.8.2 SNMP (Simple Network Management Protocol) 1250
24.8.2.1 Wie Sie alle Communities anzeigen 1252
24.8.2.2 Wie Sie eine Community hinzufügen 1253
24.8.2.3 Wie Sie eine Community ändern 1253
24.8.2.4 Wie Sie eine Community löschen 1254
24.8.2.5 Wie Sie Traps anzeigen 1254
24.8.2.6 Wie Sie Details eines Traps anzeigen 1255
24.8.3 Manuelle Aktionen 1256
24.8.3.1 Wie Sie Diagnosedaten / Diagnose-Protokolle herunterladen 1258
24.8.4 Traces 1259
24.8.4.1 Wie Sie eine Systemtrace-Protokolldatei herunterladen 1266
24.8.4.2 Wie Sie eine Systemtrace-Protokolldatei löschen 1267
24.8.4.3 Wie Sie alle Trace-Profile anzeigen 1267
24.8.4.4 Wie Sie ein Trace-Profil starten oder stoppen 1268
24.8.4.5 Wie Sie die Trace-Format-Konfiguration anzeigen oder ändern 1269
24.8.4.6 Wie Sie die Trace-Ausgabe-Interfaces anzeigen oder ändern 1269
24.8.4.7 Wie Sie das Event Viewer-Protokoll / Kunden-Trace-Protokoll anzeigen oder ändern 1270
24.8.4.8 Wie Sie das Event Viewer-Protokoll / Kunden-Trace-Protokoll herunterladen oder öffnen . . . 1270
24.8.4.9 Wie Sie das Event Viewer-Protokoll / Kunden-Trace-Protokoll löschen 1271
24.8.4.10 Wie Sie M5T-Trace-Komponenten anzeigen 1271
24.8.4.11 Wie Sie eine M5T-Trace-Komponente starten oder stoppen 1272
24.8.4.12 Wie Sie M5T-Trace-Komponenten ändern 1272
24.8.4.13 Wie Sie den Secure Trace starten oder stoppen 1273
24.8.4.14 Wie Sie den Status des Secure Trace abfragen 1273
24.8.4.15 Wie Sie das Passwort für den Secure Trace ändern 1274
24.8.4.16 Wie Sie das Zertifikat für den Secure Trace aus einer X.509-Datei importieren 1274
24.8.4.17 Wie Sie die H.323-Stack-Trace-Konfiguration anzeigen oder ändern 1275
24.8.4.18 Wie Sie H.323-Module ändern 1275
24.8.4.19 Wie Sie das H.323-Stack-Trace-Protokoll herunterladen oder öffnen 1276
24.8.4.20 Wie Sie das H.323-Stack-Trace-Protokoll löschen 1276
24.8.4.21 Wie Sie den Lizenz-Komponenten-Trace ändern 1277

24.8.4.22 Wie Sie Details eines Trace-Profils anzeigen . . . 1277
24.8.4.23 Wie Sie alle Trace-Profile stoppen . . . 1278
24.8.4.24 Wie Sie ein Trace-Profil hinzufügen . . . 1278
24.8.4.25 Wie Sie Trace-Komponenten anzeigen . . . 1278
24.8.4.26 Wie Sie Details einer Trace-Komponente anzeigen . . . 1279
24.8.4.27 Wie Sie eine Trace-Komponente starten oder stoppen . . . 1279
24.8.4.28 Wie Sie alle Trace-Komponenten stoppen . . . 1280
24.8.4.29 Wie Sie Trace-Komponenten ändern . . . 1280
24.8.5 TCP-Dump . . . 1281
24.8.5.1 Wie Sie einen TCP-Dump starten . . . 1281
24.8.5.2 Wie Sie einen TCP-Dump stoppen . . . 1281
24.8.5.3 Wie Sie einen TCP-Dump löschen . . . 1282
24.8.6 RPCAP-Dämon . . . 1282
24.8.6.1 Wie Sie den RPCAP-Dämon aktivieren . . . 1283
24.8.6.2 Wie Sie den RPCAP-Dämon deaktivieren . . . 1283
24.8.7 Events . . . 1283
24.8.7.1 Wie Sie die Event-Protokollierung über LAN ändern . . . 1286
24.8.7.2 Wie Sie eine Event-Protokolldatei herunterladen . . . 1286
24.8.7.3 Wie Sie eine Event-Protokolldatei löschen . . . 1286
24.8.7.4 Wie Sie E-Mail-Einstellungen für Events ändern . . . 1287
24.8.7.5 Wie Sie die Event-Reaktionstabelle anzeigen . . . 1287
24.8.7.6 Wie Sie Reaktionseinstellungen eines Events ändern . . . 1288
24.8.7.7 Wie Sie Reaktionseinstellungen mehrerer Events ändern . . . 1289
24.8.7.8 Wie Sie Diagnose Logs herunterladen oder öffnen . . . 1290
24.8.7.9 Wie Sie Diagnose Logs löschen . . . 1290
24.8.7.10 Wie Sie die Ziele für die Alarm-Signalisierung festlegen . . . 1290
24.8.8 Konfigurationsdaten für die Diagnose . . . 1291
24.8.8.1 Wie Sie Konfigurationsdaten für die Diagnose erzeugen . . . 1292
24.8.9 Card Manager . . . 1293
24.8.9.1 Wie Sie mit dem Card Manager die Kommunikationssoftware auf die SDHC-Karte schreiben 1294
24.9 Überwachung und Wartung der UC Suite . . . 1297
24.9.1 Protokollierung . . . 1297
24.9.1.1 Wie Sie die Aufzeichnung der Systemprotokolle aktivieren oder deaktivieren . . . 1298
24.9.1.2 Wie Sie die Aufzeichnung der Client-Logs systemweit aktivieren oder deaktivieren . . . 1299
24.9.1.3 Wie Sie die Aufzeichnung der Client-Logs teilnehmerindividuell aktivieren oder deaktivieren 1300
24.9.1.4 Wie Sie den Ablagepfad für Client-Log-Dateien konfigurieren . . . 1300
24.9.1.5 Wie Sie das zentrale Speichern der Client-Logs auf der Festplatte aktivieren oder deaktivieren . . . 1301
24.9.1.6 Wie Sie Client Logs aller internen Teilnehmer herunterladen . . . 1302
24.9.2 Benachrichtigung . . . 1302
24.9.2.1 Wie Sie E-Mail-Benachrichtigungen bei Systemfehlern konfigurieren . . . 1305
24.9.3 Wartung . . . 1306
24.9.3.1 Wie Sie die Tageszeit für die Wartung konfigurieren . . . 1307
24.9.3.2 Wie Sie die Aufbewahrungszeit für Protokolldateien konfigurieren . . . 1307
24.9.3.3 Wie Sie eine sofortige Systemwartung durchführen . . . 1308
24.9.3.4 Wie Sie die Aufbewahrungszeit für Contact-Center-Daten konfigurieren . . . 1308
24.10 Überwachung der UC Smart . . . 1309
24.10.1 Wie Sie den aktuellen Status der UC Smart abrufen . . . 1309
24.11 Remote Services . . . 1309
24.11.1 RSP.servicelink und SSDP V1 . . . 1310

24.11.1.1 Primären Remote-Service festlegen . . . 1313
24.11.1.2 Wie Sie das RSP Service-Plugin installieren, konfigurieren und registrieren . . . 1313
24.11.1.3 Wie Sie das SSDP Service-Plugin konfigurieren und registrieren . . . 1314
24.11.1.4 Wie Sie das RSP Service-Plugin aktivieren . . . 1316
24.11.1.5 Wie Sie das SSDP Service-Plugin aktivieren . . . 1317
24.11.1.6 Wie Sie das Service-Plugin deaktivieren . . . 1317
24.11.1.7 Wie Sie das RSP Service-Plugin zurücksetzen . . . 1318
24.11.1.8 Wie Sie das SSDP Service-Plugin zurücksetzen . . . 1318
24.11.1.9 Wie Sie die Partner ID des SSDP Service-Plugins ändern . . . 1319
24.11.1.10 Wie Sie den Fernzugriff auf LAN-Geräte hinzufügen oder löschen (nur für SSDP) . . . 1319
24.11.1.11 Wie Sie eine PIN für die Aktivierung und Deaktivierung des Service-Plugin konfigurieren . 1320
24.11.2 Remote-Zugang . . . 1321
24.11.2.1 Wie Sie den Remote-Zugang über ISDN einschalten . . . 1322
24.11.2.2 Wie Sie einen PC mit Microsoft Windows Vista für Remote-Zugang über ISDN konfigurieren . . . 1322
24.11.2.3 Wie Sie einen PC mit Microsoft Windows 7 für Remote-Zugang über ISDN konfigurieren . . 1324
24.11.2.4 Wie Sie den Remote-Zugang über Internet-Zugang mit fester IP-Adresse einschalten 1325
24.11.2.5 Wie Sie den Remote-Zugang über Internet-Zugang ohne feste IP-Adresse einschalten . . . 1326
24.11.2.6 Wie Sie den Remote-Zugang ausschalten . . . 1327
24.11.3 Online-Benutzer . . . 1328
24.11.3.1 Wie Sie Online-Benutzer starten . . . 1328

25 Migration . . . 1330
25.1 Lizenzmigration . . . 1332
25.2 Migration eines HiPath 3000 V9 Standalone-Systems . . . 1335
25.2.1 Wie Sie den KDS aus HiPath 3000 V9 laden . . . 1337
25.2.2 Wie Sie die HG1500 Einstellungen auslesen . . . 1337
25.2.3 Wie Sie den HiPath 3000 V9 KDS konvertieren . . . 1338
25.2.4 Wie Sie die Hardware bei HiPath 3300/3500 austauschen . . . 1338
25.2.5 Wie Sie die Hardware bei HiPath 3350/3550 austauschen . . . 1340
25.2.6 Wie Sie die Hardware bei HiPath 3800 austauschen . . . 1341
25.2.7 Wie Sie die Erstinstallation durchführen . . . 1343
25.2.8 Wie Sie den konvertierten KDS in das neue System laden . . . 1343
25.2.9 Wie Sie eine neue Lizenzdatei generieren . . . 1344
25.2.10 Wie Sie die Lizenzdatei offline aktivieren . . . 1346
25.2.11 Wie Sie Lizenzen zuordnen . . . 1346
25.2.12 Wie Sie die LCR-Einträge zurücksetzen . . . 1346
25.3 Migration eines HiPath 3000 V9 Standalone-Systems mit OpenScape Office V3 HX . . . 1346
25.3.1 Wie Sie ein OpenScape Office V3 HX Backup-Set konvertieren . . . 1348
25.4 Migration eines HiPath 3000 V9 Systems auf OpenScape Business UC Booster . . . 1349
25.4.1 Wie Sie UC Booster manuell aktivieren . . . 1350
25.5 Migration eines HiPath 3000 V9 Netzverbunds . . . 1354
25.6 Migration eines HiPath 3000 V9 Netzverbunds mit HiPath 5000 RSM . . . 1357
25.7 Migration eines HiPath 3000 V9 Netzverbunds mit OpenScape Office LX . . . 1359
25.8 Geänderte Leistungsmerkmale und Schnittstellen . . . 1362
25.9 Nicht unterstützte Baugruppen und Endgeräte . . . 1367
25.9.1 Wie Sie ein optiPoint WL2 professional von HFA auf SIP umrüsten . . . 1372

26 Ausbaugrenzen und Kapazitäten . . . 1374
26.1 Systembedingte Ausbaugrenzen . . . 1374

26.2 Software-Kapazitäten 1379

27 Experten-Modus 1392
27.1 Darstellungskonventionen für Parameterbeschreibungen 1392
27.2 Wartung 1393
27.2.1 Konfiguration. 1393
27.2.1.1 Konfiguration > Wartemusik (MoH) > Laden zum Gateway 1393
27.2.1.2 Konfiguration > Ansagen > Laden zum Gateway 1394
27.2.1.3 Konfiguration > Port-Konfiguration 1394
27.2.1.4 Konfiguration > SmartVM 1395
27.2.1.5 Konfiguration > SmartVM > Mailbox-Operationen 1395
27.2.1.6 Konfiguration > SmartVM > Dateioperationen 1396
27.2.1.7 Konfiguration > Branding 1398
27.2.1.8 Konfiguration > IP-Gateway-Adresse 1398
27.2.2 Software-Image 1399
27.2.2.1 Software-Image > System-Software > Update via Internet 1399
27.2.2.2 Software-Image > System-Software > Update via File Upload 1400
27.2.2.3 Software-Image > System-Software > Update via USB Stick 1400
27.2.2.4 Software-Image > Telefon-Images > Laden 1401
27.2.2.5 Software-Image > Telefon-Images > Verteilen 1401
27.2.2.6 Software-Image > Telefon-Images > Verteilen pro Endgerät 1402
27.2.2.7 Software-Image > Telefon-Logo-Images > Laden. 1402
27.2.2.8 Software-Image > Telefon-Logo-Images > Verteilen 1403
27.2.3 Cordless 1403
27.2.3.1 Cordless > Basisstationen 1403
27.2.4 Port/Baugruppen Zustand. 1405
27.2.4.1 Port/Baugruppen Zustand > Baugruppen Zustand 1405
27.2.4.2 Port/Baugruppen Zustand > Out of Service 1406
27.2.5 Traces. 1407
27.2.5.1 Traces > Trace-Format-Konfiguration 1407
27.2.5.2 Traces > Trace-Ausgabe-Interfaces 1408
27.2.5.3 Traces > Trace- Protokoll 1409
27.2.5.4 Traces > Digitale Prüfschleife 1409
27.2.5.5 Traces > Kunden-Trace-Protokoll 1409
27.2.5.6 Traces > M5T-Trace-Komponenten 1410
27.2.5.7 Traces > Secure Trace 1410
27.2.5.8 Traces > Secure Trace > Secure Trace-Zertifikat 1411
27.2.5.9 Traces > Secure Trace > Secure Trace-Einstellungen 1411
27.2.5.10 Traces > Call Monitoring 1412
27.2.5.11 Traces > H.323-Stack-Trace 1414
27.2.5.12 Traces > Lizenz-Komponente 1415
27.2.5.13 Traces > Trace-Profile. 1416
27.2.5.14 Traces > Trace-Komponenten. 1416
27.2.5.15 Traces > TCP- Dump 1417
27.2.5.16 Traces > rpcap Dämon 1417
27.2.6 Events. 1418
27.2.6.1 Events > Event-Konfiguration 1418
27.2.6.2 Events > Event-Protokoll. 1419
27.2.6.3 Events > E-Mail 1419
27.2.6.4 Events > Reaktionstabelle. 1419
27.2.6.5 Events > Diagnose Logs 1420
27.2.6.6 Events > Alarm-Signalisierung 1421

27.2.7 Restart / Reload 1421
27.2.7.1 Restart / Reload > Restart / Reload 1422
27.2.8 SNMP 1423
27.2.8.1 SNMP > Communities 1423
27.2.8.2 SNMP > Communities > Lesende Communities 1423
27.2.8.3 SNMP > Communities > Schreibende Communities 1424
27.2.8.4 SNMP > Communities > Trap Communities 1424
27.2.8.5 SNMP > Traps 1424
27.2.9 Admin-Protokoll 1425
27.2.9.1 Admin-Protokoll > Konfiguration 1425
27.2.9.2 Admin-Protokoll > Admin.-Protokoll-Daten 1425
27.2.10 Aktionen 1426
27.2.10.1 Aktionen > Manuelle Aktionen > Diagnose-Protokolle 1426
27.2.10.2 Aktionen > Automatische Aktionen > Garbage Collection 1427
27.2.10.3 Aktionen > Automatische Aktionen > DLS Notification 1428
27.2.11 Plattform-Diagnose 1428
27.2.12 Applikat.-Diagnose 1428
27.2.12.1 Applikat.-Diagnose > Entwickler-Einstellungen > Trace-Konsolen-Ausgabe 1429
27.2.12.2 Applikat.-Diagnose > Entwickler-Einstellungen > Übernahme des Write Tokens 1429
27.2.12.3 Applikat.-Diagnose > Mainboard 1429
27.2.13 IP-Diagnose 1429
27.2.13.1 IP-Diagnose > Mainboard > ARP-Protokoll 1429
27.2.13.2 IP-Diagnose > Mainboard > ICMP-Anforderung > Ping 1429
27.2.13.3 IP-Diagnose > Mainboard > ICMP-Anforderung > Traceroute 1430
27.2.14 Online-Benutzer 1430
27.2.14.1 Online Benutzer 1430
27.3 Telefonie 1431
27.3.1 Grundeinstellungen 1431
27.3.1.1 Grundeinstellungen > System > System Flags 1431
27.3.1.2 Grundeinstellungen > System > Zeitparameter 1436
27.3.1.3 Grundeinstellungen > System > Display 1442
27.3.1.4 Grundeinstellungen > System > DISA 1444
27.3.1.5 Grundeinstellungen > System > Abwurf/VPL/Hotline 1445
27.3.1.6 Grundeinstellungen > System > LDAP 1448
27.3.1.7 Grundeinstellungen > System > Texts 1449
27.3.1.8 Grundeinstellungen > System > Flexible Menüs 1450
27.3.1.9 Grundeinstellungen > System > Kurzwahlziele 1450
27.3.1.10 Grundeinstellungen > System > Servicekennzahlen 1451
27.3.1.11 Grundeinstellungen > Gateway 1451
27.3.1.12 Grundeinstellungen > DynDNS > DynDNS Service 1452
27.3.1.13 Grundeinstellungen > DynDNS > Aktualisierungszeit der DNS-Namen 1453
27.3.1.14 Grundeinstellungen > Quality of Service 1454
27.3.1.15 Grundeinstellungen > Datum und Uhrzeit > Datum und Uhrzeit 1455
27.3.1.16 Grundeinstellungen > Datum und Uhrzeit > Zeitzonen-Einstellungen 1455
27.3.1.17 Grundeinstellungen > Datum und Uhrzeit > SNTP-Einstellungen 1456
27.3.1.18 Grundeinstellungen > Port-Verwaltung 1456
27.3.1.19 Grundeinstellungen > Gebühren > Gebühren Ausgabe 1457
27.3.1.20 Grundeinstellungen > Gebühren > Gebühren Faktoren 1458
27.3.1.21 Grundeinstellungen > Gebühren > Gebühren Projekt Kennzahlen 1459
27.3.1.22 Grundeinstellungen > Wiedergabegerät für Sprachnachrichten/Ansagen 1460
27.3.1.23 Grundeinstellungen > Telefonparameter-Bereitstellung 1460
27.3.1.24 Grundeinstellungen > Power Management 1461

27.3.2 Sicherheit 1462
27.3.2.1 Sicherheit > Application Firewall 1462
27.3.2.2 Sicherheit > Deployment- und Licensing-Client (DLSC) 1463
27.3.2.3 Sicherheit > Deployment- und Licensing-Client (DLSC) > DLSC-Client-Zertifikat 1463
27.3.2.4 Sicherheit > Deployment- und Licensing-Client (DLSC) > DLSC-CA-Zertifikat 1464
27.3.2.5 Sicherheit > Signaling- und Payload-Encryption 1465
27.3.2.6 Sicherheit > Signaling- und Payload-Encryption > SPE Zertifikat 1466
27.3.2.7 Sicherheit > Signaling- und Payload-Encryption > SPE CA Zertifikate 1467
27.3.2.8 Sicherheit > VPN 1467
27.3.2.9 Sicherheit > VPN > Lightweight CA 1468
27.3.2.10 Sicherheit > VPN > Zertifikatsverwaltung 1468
27.3.2.11 Sicherheit > VPN > Zertifikatsverwaltung > Trusted CA Zertifikate > Aktive Zertifikate 1469
27.3.2.12 Sicherheit > VPN > Zertifikatsverwaltung > Trusted CA Zertifikate > Konfigurierte Zertifikate 1470
27.3.2.13 Sicherheit > VPN > Peer-Zertifikate 1470
27.3.2.14 Sicherheit > VPN > Dienste > Aktive Dienste 1472
27.3.2.15 Sicherheit > VPN > Dienste > Konfigurierte Dienste 1472
27.3.2.16 Sicherheit > VPN > Tunnel > Aktive Tunnel 1473
27.3.2.17 Sicherheit > VPN > Tunnel > Konfigurierte Tunnel 1475
27.3.2.18 Sicherheit > VPN > Regeln > Aktive Regeln 1479
27.3.2.19 Sicherheit > VPN > Regeln > Konfigurierte Regeln 1480
27.3.2.20 Sicherheit > VPN > Public Key Infrastructure (PKI) 1481
27.3.2.21 Sicherheit > SSL > Zertifikatsgenerierung 1481
27.3.2.22 Sicherheit > SSL > Zertifikatsverwaltung 1483
27.3.2.23 Sicherheit > SSL > Zertifikatsverwaltung > Server-Zertifikate 1483
27.3.2.24 Sicherheit > Web Sicherheit 1484
27.3.3 Netzwerkschnittstellen 1485
27.3.3.1 Netzwerkschnittstellen > Mainboard > Host-Name 1485
27.3.3.2 Netzwerkschnittstellen > Mainboard > LAN 1 (WAN) 1485
27.3.3.3 Netzwerkschnittstellen > Mainboard > LAN 2 1489
27.3.3.4 Netzwerkschnittstellen > Mainboard > LAN 3 (Admin) 1490
27.3.3.5 Netzwerkschnittstellen > Mainboard > FTP-Server 1491
27.3.3.6 Netzwerkschnittstellen > Mainboard > DHCP Modus 1491
27.3.3.7 Netzwerkschnittstellen > Mainboard > DHCP Modus > DHCP-Server > Globale Parameter . 1492
27.3.3.8 Netzwerkschnittstellen > Mainboard > DHCP Modus > DHCP-Server > IP-Adressen-Pools . 1493
27.3.3.9 Netzwerkschnittstellen > Mainboard > DHCP Modus > DHCP-Server > Statische IP-Adressen 1494
27.3.3.10 Netzwerkschnittstellen > Mainboard > DHCP Modus > DHCP-Server > Zuletzt aktive Leases 1495
27.3.3.11 Netzwerkschnittstellen > Mainboard > DHCP Modus > DHCP-Server > Alle Leases 1496
27.3.3.12 Netzwerkschnittstellen > Applicationboard > Host-Name 1496
27.3.3.13 Netzwerkschnittstellen > Applicationboard > LAN 1 1496
27.3.3.14 Netzwerkschnittstellen > Applicationboard > LAN 2 1497
27.3.4 Routing 1498
27.3.4.1 Routing > IP-Routing > Mainboard > Statische Routen 1498
27.3.4.2 Routing > IP-Routing > Mainboard > Default Router 1499
27.3.4.3 Routing > IP-Routing > Mainboard > DNS-Server 1499
27.3.4.4 Routing > IP-Routing > Applicationboard > Statische Routen 1500
27.3.4.5 Routing > IP-Routing > Applicationboard > Default Router 1500
27.3.4.6 Routing > NAT 1501
27.3.4.7 Routing > PSTN 1502
27.3.4.8 Routing > PSTN > PPP-Protokoll 1502

27.3.4.9 Routing > PSTN > PSTN-Partner 1502
27.3.5 LCR 1506
27.3.5.1 LCR > LCR-Flags 1506
27.3.5.2 LCR > Classes Of Service 1507
27.3.5.3 LCR > Wahlplan 1507
27.3.5.4 LCR > Wegetabelle 1508
27.3.5.5 LCR > Wahlregel 1509
27.3.6 Sprachgateway 1511
27.3.6.1 Sprachgateway > SIP-Parameter 1511
27.3.6.2 Sprachgateway > Codec-Parameter 1512
27.3.6.3 Sprachgateway > Ziel-Codec-Parameter 1514
27.3.6.4 Sprachgateway > Internet-Telefonie Service Provider 1514
27.3.6.5 Sprachgateway > Networking > Knoten 1518
27.3.6.6 Sprachgateway > Networking > Routing 1518
27.3.6.7 Sprachgateway > SIPQ-Verbindung 1519
27.3.7 Teilnehmer 1520
27.3.7.1 Teilnehmer > Teilnehmer > UP0 Teilnehmer 1520
27.3.7.2 Teilnehmer > Teilnehmer > IP Clients 1523
27.3.7.3 Teilnehmer > Teilnehmer > Analoge Teilnehmer 1524
27.3.7.4 Teilnehmer > Teilnehmer > ISDN Teilnehmer 1525
27.3.7.5 Teilnehmer > Teilnehmer > DECT-Teilnehmer > Basestations 1526
27.3.7.6 Teilnehmer > Teilnehmer > DECT-Teilnehmer > DECT Teilnehmer 1527
27.3.7.7 Teilnehmer > Teilnehmer > IVM/EVM Ports > IVM 1528
27.3.7.8 Teilnehmer > Teilnehmer > IVM/EVM Ports > EVM 1528
27.3.7.9 Teilnehmer > Teilnehmer > Virtuelle Teilnehmer 1529
27.3.7.10 Teilnehmer > Teilnehmer > Teilnehmer-Parameter 1530
27.3.7.11 Teilnehmer > Teilnehmer > Applikation-Suite 1539
27.3.7.12 Teilnehmer > Teilnehmer > Profile/Vorlagen 1540
27.3.7.13 Teilnehmer > Teilnehmer > Durchwahl Rufnummern 1541
27.3.7.14 Teilnehmer > Teilnehmer > Mobility Entry 1542
27.3.7.15 Teilnehmer > Teilnehmer > Übersicht Teilnehmer 1543
27.3.7.16 Teilnehmer > Tastenprogrammierung 1544
27.3.8 Cordless 1544
27.3.8.1 Cordless > Systemweit 1544
27.3.8.2 Cordless > SLC 1546
27.3.8.3 Cordless > Multi-SLC 1547
27.3.8.4 Cordless > Basisstationen 1548
27.3.9 Kommende Rufe 1548
27.3.9.1 Kommende Rufe > Gruppen-/Sammelanschluss 1549
27.3.9.2 Kommende Rufe > Gruppen-Teilnehmer 1551
27.3.9.3 Kommende Rufe > Team/Top 1552
27.3.9.4 Kommende Rufe > Anrufübernahme 1555
27.3.9.5 Kommende Rufe > UCD 1556
27.3.9.6 Kommende Rufe > Rufweiterschaltungen 1558
27.3.10 Leitungen/Vernetzung 1560
27.3.10.1 Leitungen/Vernetzung > Leitungen 1561
27.3.10.2 Leitungen/Vernetzung > Richtung 1563
27.3.10.3 Leitungen/Vernetzung > QSIG-Leistungsmerkmale 1570
27.3.10.4 Leitungen/Vernetzung > MSN zuweisen 1571
27.3.10.5 Leitungen/Vernetzung > ISDN-Parameter 1571
27.3.11 Berechtigungen 1572
27.3.11.1 Berechtigungen > Teilnehmer 1572

27.3.11.2 Berechtigungen > Tag: Berechtigungsgruppen . . . 1573
27.3.11.3 Berechtigungen > Nacht: Berechtigungsgruppen . . . 1573
27.3.11.4 Berechtigungen > Erlaubnislisten . . . 1574
27.3.11.5 Berechtigungen > Verbotslisten . . . 1575
27.3.11.6 Berechtigungen > Nachtschaltung . . . 1575
27.3.11.7 Berechtigungen > VBZ Gruppenzuordnung . . . 1576
27.3.11.8 Berechtigungen > VBZ Matrix . . . 1576
27.3.11.9 Berechtigungen > Automatische Nachtschaltung . . . 1577
27.3.11.10 Berechtigungen > Sondertage . . . 1578
27.3.12 Anschaltungen . . . 1578
27.3.12.1 Anschaltungen > Ansage/Interne Wartemusik > Ansagen und Wartemusik . . . 1578
27.3.12.2 Anschaltungen > Türsprechstelle . . . 1579
27.3.12.3 Anschaltungen > SmartVM . . . 1579
27.3.13 Payload . . . 1582
27.3.13.1 Payload > Devices . . . 1582
27.3.13.2 Payload > Media Stream Control (MSC) . . . 1583
27.3.13.3 Payload > HW-Module . . . 1583
27.3.14 Statistiken . . . 1586
27.3.14.1 Statistiken > Gateway-Statistk > Mainboard > Device-Statistiken . . . 1586
27.3.14.2 Statistiken > Gateway-Statistken > Mainboard > MSC-Statistiken . . . 1587
27.3.14.3 Statistiken > SNMP Statistik . . . 1587
27.3.14.4 Statistiken > Telephonie Statistiken > System Texte . . . 1587
27.3.14.5 Statistiken > Telephonie Statistiken > UCD Agenten . . . 1588
27.3.14.6 Statistiken > Telephonie Statistiken > Zustand Leitung . . . 1588
27.3.14.7 Statistiken > Telephonie Statistiken > Weiterleitung . . . 1589
27.3.14.8 Statistiken > Telephonie Statistiken > Teilnehmer . . . 1589
27.4 Applikationen . . . 1591
27.4.1 Applikationsauswahl . . . 1591
27.4.1.1 Applikationsauswahl . . . 1591
27.4.2 UC Smart . . . 1591
27.4.2.1 UC Smart > Grundeinstellungen . . . 1591
27.4.2.2 UC Smart > Benutzerverwaltung . . . 1592
27.4.2.3 UC Smart > Status . . . 1593
27.4.3 OpenScape Business UC Suite . . . 1593
27.4.3.1 OpenScape Business UC Suite . . . 1593
27.4.3.2 OpenScape Business UC Suite > Benutzerverzeichnis . . . 1594
27.4.3.3 OpenScape Business UC Suite > Abteilungen . . . 1595
27.4.3.4 OpenScape Business UC Suite > Gruppen . . . 1596
27.4.3.5 OpenScape Business UC Suite > Templates . . . 1596
27.4.3.6 OpenScape Business UC Suite > Externes Verzeichnis . . . 1597
27.4.3.7 OpenScape Business UC Suite > Externer Anbieter . . . 1597
27.4.3.8 OpenScape Business UC Suite > Contact Center . . . 1598
27.4.3.9 OpenScape Business UC Suite > Zeitpläne . . . 1605
27.4.3.10 OpenScape Business UC Suite > Datei-Upload . . . 1606
27.4.3.11 OpenScape Business UC Suite > Konferenzschaltung . . . 1607
27.4.3.12 OpenScape Business UC Suite > Standort-Liste . . . 1608
27.4.3.13 OpenScape Business UC Suite > Server . . . 1608
27.4.3.14 OpenScape Business UC Suite > Profile . . . 1612
27.4.3.15 OpenScape Business UC Suite > Faxkopfzeilen . . . 1614
27.4.3.16 OpenScape Business UC Suite > Skin-Einstellungen . . . 1614
27.4.4 Web Services . . . 1614
27.4.4.1 Web Services > XMPP . . . 1614

27.4.4.2 Web Services > Web Collaboration 1615
27.4.5 Open Directory Service 1616
27.4.5.1 Open Directory Service > Grundeinstellungen 1616
27.4.5.2 Open Directory Service > Datenquellen > OpenScape Business 1616
27.4.5.3 Open Directory Service > Datenquellen > Kurzwahlen 1616
27.4.5.4 Open Directory Service > Datenquellen > LXV3 1617
27.4.5.5 Open Directory Service > Wartung 1617
27.4.5.6 OpenStage Gate View 1617
27.4.6 OpenStage Gate View 1617
27.4.7 Application Launcher 1617
27.4.7.1 Application Launcher 1618
27.4.8 IVM 1618
27.5 Middleware 1618
27.5.1 Wiedergabegerät für Ansagen 1618
27.5.2 CSTA Message Dispatcher (CMD) 1619
27.5.3 CSTA Service Provider (CSP) 1619
27.5.4 DSS-Server 1620
27.5.5 Media Extension Bridge (MEB) 1620

28 Anhang 1621
28.1 Unterstützte Standards 1621
28.2 Euro-ISDN-Leistungsmerkmale 1623
28.3 Verwendete Ports 1625
28.4 Projektierung der DSP-Kanäle für die Kommunikationssysteme OpenScape Business X3/X5/X8 1627

29 Glossar 1636
29.1 Glossar 1636

Stichwörter 1653

1 Einführung und wichtige Hinweise

In der Einführung erhalten Sie einen Überblick über die Struktur dieser Dokumentation. Die Einführung soll Ihnen helfen, Informationen zu Themen schneller zu finden. Bevor Sie mit der Montage und Inbetriebnahme des Kommunikationssystems beginnen, beachten Sie unbedingt die Sicherheitshinweise und Warnungen und die wichtigen Hinweise.

INFO: Die Sicherheitshinweise und Warnungen informieren Sie über die zu beachtenden Sicherheits- und Warnhinweise. Die wichtigen Hinweise enthalten Angaben über das Verhalten in Notfällen, die Normen und Richtlinien bezüglich der Installation und die Funkstöreigenschaften des Kommunikationssystems. Darüber hinaus erhalten Sie Informationen zur sachgemäßen Entsorgung und zum sachgemäßen Recycling.

1.1 Über diese Dokumentation

Diese Dokumentation beschreibt die Administration von OpenScape Business™.

Enthalten Sie die Hardwareplattformen OpenScape Business X1, OpenScape Business X3, OpenScape Business X5 und OpenScape Business X8 sowie der Softswitch OpenScape Business S. Die UC Suite Funktionalität wird mit der optionalen UC Booster Card oder dem UC Booster Server geboten. Bei OpenScape Business S ist die UC Suite integriert.

INFO: Die Hardwareplattformen OpenScape Business X1/X3/X5/X8 (kurz OpenScape Business X) und der Softswitch OpenScape Business S werden in dieser Dokumentation auch als Kommunikationssysteme bezeichnet.

UC Suite bezeichnet die erweiterten Unified-Communications-Funktionen inkl. Multimedia Contact Center.

Die Informationen in dieser Dokumentation enthalten allgemeine Beschreibungen der technischen Möglichkeiten, welche im Einzelfall nicht immer vorliegen müssen. Die gewünschten Leistungsmerkmale sind im Einzelfall bei Vertragsabschluss festzulegen.

Wenn eine Funktion nicht wie beschrieben verfügbar ist, dann kann dies folgende Ursachen haben:

- Das Kommunikationssystem verfügt nicht über dieses Leistungsmerkmal.
- Die benötigte Lizenz ist nicht vorhanden oder aktiviert.

1.1.1 Dokumentationen und Zielgruppen

Die Dokumentationen zu OpenScape Business richten sich an unterschiedliche Zielgruppen.

Vertrieb und Projektplaner

- Leistungsmerkmalbeschreibung
  Diese Dokumentation beschreibt sämtliche Leistungsmerkmale und richtet sich an Vertrieb und Kunden. Dieses Dokument ist ein Auszug aus der Administratordokumentation.

Installation und Service

- Installation OpenScape Business X1, Servicedokumentation
  Diese Dokumentation beschreibt die Hardware von OpenScape Business X1 inkl. der Installation der Hardware und richtet sich an Servicetechniker.
- Installation OpenScape Business X3/X5/X8, Servicedokumentation
  Diese Dokumentation beschreibt die Hardware von OpenScape Business X3/X5/X8 inkl. der Installation der Hardware und richtet sich an Servicetechniker.
- Installation Linux-Server, Installationsanleitung
  Diese Dokumentation beschreibt die Installation von Linux auf einem separaten Server-PC als Plattform für den Softswitch OpenScape Business S und den Application Server OpenScape Business UC Booster Server und richtet sich an Administratoren.
- Installation OpenScape Business S, Installationsanleitung
  Diese Dokumentation beschreibt die Erstinstallation des Softswitchs OpenScape Business S inkl. der UC-Lösung UC Suite und richtet sich an Servicetechniker.

Administration

- Administratordokumentation
  Diese Dokumentation beschreibt die Konfiguration der Leistungsmerkmale, die über den OpenScape Business Assistant (WBM) eingerichtet werden und richtet sich an Administratoren. Die Administratordokumentation ist im System als Online-Hilfe verfügbar.
- Manager E, Administratordokumentation
  Diese Dokumentation beschreibt die Konfiguration der Leistungsmerkmale, die über den Manager E eingerichtet werden und richtet sich an Administratoren.

Communications Clients

- myPortal Smart, Bedienungsanleitung
  Diese Dokumentation beschreibt die Konfiguration und Bedienung der Applikation myPortal Smart und richtet sich an Benutzer.

- myPortal for OpenStage, Bedienungsanleitung
  Diese Dokumentation beschreibt die Konfiguration und Bedienung von myPortal for OpenStage und richtet sich an Benutzer.
- myPortal for Desktop, Bedienungsanleitung
  Diese Dokumentation beschreibt die Installation, Konfiguration und Bedienung der Applikation myPortal for Desktop und richtet sich an Benutzer.
- myPortal for Outlook, Bedienungsanleitung
  Diese Dokumentation beschreibt die Installation, Konfiguration und Bedienung der Applikation myPortal for Outlook und richtet sich an Benutzer.
- Fax Printer, Bedienungsanleitung
  Diese Dokumentation beschreibt die Installation, Konfiguration und Bedienung von Fax Printer und richtet sich an Benutzer.

Mobile Clients

- myPortal for Mobile/Tablet, Bedienungsanleitung
  Diese Dokumentation beschreibt die Konfiguration und Bedienung von myPortal for Mobile für Mobiltelefone und Tablet-PC und richtet sich an Benutzer.
- myPortal to go, Bedienungsanleitung
  Diese Dokumentation beschreibt die Konfiguration und Bedienung von myPortal to go für Smartphones und richtet sich an Benutzer.

Contact Center Clients

- myAgent, Bedienungsanleitung
  Diese Dokumentation beschreibt die Installation, Konfiguration und Bedienung der Applikation myAgent und richtet sich an Benutzer.
- myReports, Bedienungsanleitung
  Diese Dokumentation beschreibt die Installation, Konfiguration und Bedienung der Applikation myReports und richtet sich an Benutzer.

Attendants

- myAttendant, Bedienungsanleitung
  Diese Dokumentation beschreibt die Installation, Konfiguration und Bedienung des Vermittlungsplatzes myAttendant und richtet sich an Benutzer.
- OpenScape Business Attendant, Bedienungsanleitung
  Diese Dokumentation beschreibt die Installation, Konfiguration und Bedienung des Vermittlungsplatzes OpenScape Business Attendant und richtet sich an Benutzer.

Telefon User Interfaces (TUIs)

- UC Smart Telefon User Interface (TUI), Kurzbedienungsanleitung
  Diese Dokumentation beschreibt die Telefonmenüs der Sprachbox (UC Smart) und richtet sich an Benutzer.
- UC Suite Telefon User Interface (TUI), Kurzbedienungsanleitung
  Diese Dokumentation beschreibt das Telefonmenü der Sprachbox (UC Suite) und richtet sich an Benutzer.

1.1.2 Gliederung Administratordokumentation

Die Gliederung zeigt Ihnen die inhaltliche Struktur der Administratordokumentation. Die Beschreibung der Hardware finden Sie in der Servicedokumentation.

Kapitel	Inhalt
Einführung und wichtige Hinweise	Überblick über die Struktur dieser Dokumentation und wichtige Hinweise/Sicherheitshinweise für Installation und Betrieb
Systemüberblick	Überblick über das Kommunikationssystem für einen schnellen Einstieg
Administrationskonzept	Überblick über die Administrationsprogramme und die Benutzerrollen im WBM
Erstinstallation OpenScape Business X	Integration von OpenScape Business X3/X5/X8 ins Kunden-LAN und Basiskonfiguration über Wizards
Erstinstallation OpenScape Business S	Integration von OpenScape Business S ins Kunden-LAN und Basiskonfiguration über Wizards
Erstinstallation OpenScape Business UC_Booster	Integration von OpenScape Business UC Booster ins Kunden-LAN und Basiskonfiguration über Wizards
Lizenzierung	Lizenzierungsverfahren und Lizenzen
Integration ins interne Datennetz (LAN)	LAN/WAN-Schnittstelle, Namensauflösung, Daten-Routing, DLI und DLS
Anbindung an Service-Provider	Internet-Zugang, IP-Telefonie, Amtszugang
Teilnehmer	Rufnummernplan, IP-Teilnehmer, UP0-Teilnehmer; DECT-Teilnehmer, ISDN und analoge Teilnehmer, Virtuelle Teilnehmer, Benutzer der UC Clients, Benutzerprofile
UC Smart	Clients und Funktionen der Unified-Communications-Lösung UC Smart inkl. Smart VoiceMail. Anwesenheitsstatus, Verzeichnisse und Journal, Konferenzen, Team-Funktionen, Sprachnachrichten
UC Suite	Clients und Funktionen der Unified-Communications-Lösung UC Suite: Anwesenheitsstatus und CallMe, Verzeichnisse und Journal, Konferenzen und Web Collaboration, Sprach- und Faxnachrichten, Instant Messaging
Funktionen am Telefon	Anrufen, Anrufsignalisierung, Rufnummernanzeige, Funktionen während der Verbindung, Optimieren der Kommunikationsabläufe
Arbeiten im Team (Gruppen)	Anrufübernahmegruppe, Gruppenruf, Sammelanschluss, Team/Top, MULAP, UCD
Anruf-Routing	Berechtigungen, Wahlkontrolle, Gemeinschaftsanlage, LCR, Notrufe

Kapitel	Inhalt
Attendants	AutoAttendants, OpenStage Attendant, PC-basierte Attendants, Abwurfplatz
Multimedia Contact Center	Clients und Funktionen des Contact Centers: Agenten, Warteschlangen und Zeitpläne, VIP-Betreuung, Fallback, Berichte
Mobility	myPortal for Mobile/Tablet, myPortal to go, Mobility Entry, One Number Service, Dual-Mode-Telefonie, IP-Mobility, Cordless/DECT
Security	Firewall, SPE, VPN, Zertifikate
Vernetzung von OpenScape Business	Vernetzungsplan, Vernetzungsszenarien, Zentraler Abwurfplatz, Survivability
Anschaltungen	Ansagegeräte, Türsprechstelle und Türöffner, Aktoren und Sensoren, OpenStage Gate View
Application Connectivity	CSTA, TAPI, XMPP, Application Launcher
Accounting	Gesprächsdatenerfassung, Gebühren und Gesprächsdauer, Kostenkontrolle
Maintenance	Sichern und Wiederherstellen, Update, Restart, Reload, Shutdown, Factory Reset, Inventory, Aktionen, Remote Services
Migration	Hochrüsten von HiPath 3000 auf OpenScape Business
Ausbaugrenzen und Kapazitäten	Maximalwerte für die Ausbaugrenzen und Kapazitäten der unterschiedlichen Kommuniktionssysteme
Experten-Modus	Referenzbeschreibung der Fenster/Masken des Experten-Modus
Anhang	Auflistung der unterstützten Standards, der Euro-ISDN-Leistungsmerkmale und der verwendeten IP-Protokolle und Portnummern
Glossar	Kurzbeschreibungen allgemeiner Begriffe

Verwandte Themen

- Gliederung Servicedokumentation

1.1.3 Gliederung Servicedokumentation

Die Gliederung zeigt Ihnen die inhaltliche Struktur der Servicedokumentation. Informationen über die Erstinstallation und die Konfiguration finden Sie in der Administratordokumentation.

Kapitel	Inhalt
Einführung und wichtige Hinweise	Überblick über die Struktur dieser Dokumentation, Sicherheits und Warnhinweise und Hinweise über das Verhalten in Notfällen, den bestimmungsgemäßen Gebrauch und die Betriebsbedingungen der Kommunikationssysteme und Server
Kommunikationssysteme	Beschreibung der Kommunikationssysteme OpenScape Business X3R, X3W, X5R, X5W und X8
Baugruppen	Übersicht und Beschreibung der bestellbaren Baugruppen
Montage OpenScape Business X3R und OpenScape Business X5R (19"-Rackgehäuse)	Vorgehensweise bei der Standardmontage: Voraussetzungen, vorbereitende Tätigkeiten, Montagearten, Schutzerdung, Konfigurationshinweise, Amtsanschluss, Anschluss von Telefonen und Geräten, abschließende Tätigkeiten
Montage OpenScape Business X3W und OpenScape Business XW (Wandgehäuse)	Vorgehensweise bei der Standardmontage: Voraussetzungen, vorbereitende Tätigkeiten, Montageart, Hauptverteiler MDFU, Schutzerdung, Verbindungs- und Anschlusskabel, Konfigurationshinweise, Amtsanschluss, Anschluss von Telefonen und Geräten, Störausstrahlung, abschließende Tätigkeiten
Montage OpenScape Business X8	Vorgehensweise bei der Standardmontage: Voraussetzungen, vorbereitende Tätigkeiten, Montagearten, Hauptverteiler MDFU-E, Patch-Panels, Schutzerdung, Konfigurationshinweise, Backplanes der Systemboxen, Amtsanschluss, Anschluss von Telefonen und Geräten, abschließende Tätigkeiten
Erweiterungen	Angaben zum Anschluss von Zusatzgeräten
Integrierte Cordless-Lösung	Systemausbau und Ausbaugrenzen, Basisstationen und deren Montage, Vorgaben für die Projektierung
Anhang	Hardware-Ausbau, Schnittstellen-Reichweiten, Leitungslängen, länderabhängige Ruffrequenzen

Verwandte Themen

- Gliederung Administratordokumentation

1.1.4 Arten von Themen

Die Arten von Themen umfassen Konzepte und Tasks:

Art des Themas	Beschreibung
Konzept	Erklärt das "Was" und gibt einen Überblick über Zusammenhänge sowie Hintergrundinformationen z. B. zu Leistungsmerkmalen.
Task (Handlungsanweisung)	Beschreibt das "Wie" für aufgabenorientierte Anwendungsfälle Schritt für Schritt das und setzt Kenntnis der zugehörigen Konzepte voraus. Tasks sind erkennbar an der Überschrift **Wie Sie ...**.

1.1.5 Darstellungskonventionen

Diese Dokumentation verwendet unterschiedliche Mittel zur Darstellung verschiedener Arten von Informationen.

Art der Information	Darstellung	Beispiel
Elemente der Benutzeroberfläche	fett	Klicken Sie auf **OK**.
Menüfolge	>	**Datei > Beenden**
Besondere Hervorhebung	fett	**Name** darf nicht gelöscht werden
Querverweistext	kursiv	Weitere Informationen finden Sie im Themenbereich *Netzwerk*.
Ausgabe	Schriftart mit fester Laufweite, z. B. Courier	`Befehl nicht gefunden.`
Eingabe	Schriftart mit fester Laufweite, z. B. Courier	`LOCAL` als Dateiname eingeben
Tastenkombination	Schriftart mit fester Laufweite, z. B. Courier	`<Strg>+<Alt>+<Esc>`

1.2 Sicherheits- und Warnhinweise

Sicherheits- und Warnhinweise kennzeichnen Situationen, die Tod, schwere Verletzungen, Sachschäden und/oder Datenverlust zur Folge haben können.

Arbeiten an Kommunikationssystemen und Geräten dürfen **nur** von qualifizierten Personen durchgeführt werden.

Im Kontext dieser Sicherheits- und Warnhinweise sind qualifizierte Personen definiert als Personen, die autorisiert sind, Systeme, Geräte und Leitungen gemäß den geltenden Sicherheitsvorgehensweisen und -standards in Betrieb zu nehmen, zu erden und zu beschriften.

Lesen und beachten Sie unbedingt die nachfolgenden Sicherheits- und Warnhinweise, bevor Sie mit der Montage und Inbetriebnahme des Kommunikationssystems beginnen.

Lesen Sie darüber hinaus alle Sicherheits- und Warnhinweise auf dem Kommunikationssystem und den Geräten sorgfältig durch, und befolgen Sie diese.

Informieren Sie sich auch über die Notrufnummern.

Arten von Sicherheits- und Warnhinweisen

In dieser Dokumentation werden folgende Abstufungen der Sicherheits- und Warnhinweise verwendet:



GEFAHR

Kennzeichnet unmittelbar gefährliche Situation, die Tod oder schwere Verletzungen zur Folge haben wird.



WARNUNG

Kennzeichnet allgemein gefährliche Situation, die Tod oder schwere Verletzungen zur Folge haben kann.



VORSICHT

Kennzeichnet gefährliche Situation, die Verletzungen zur Folge habe kann.

HINWEIS: Kennzeichnet Situationen, die Sachschäden und/oder Datenverlust zur Folge haben können.

Weitere Symbole zur näheren Bestimmung der Gefahrenquelle

Das folgende Symbol wird in der Regel nicht in der vorliegenden Dokumentation verwendet, sondern kann auf Geräten oder Verpackungen abgebildet sein.



EGB Elektrostatisch gefährdete Bauelemente

Verwandte Themen

- Wichtige Hinweise

1.2.1 Warnhinweise: Gefahr

Warnhinweise des Typs Gefahr kennzeichnen eine unmittelbar gefährliche Situation, die Tod oder schwere Verletzungen zur Folge haben wird.



GEFAHR

Elektrischer Schlag durch Berühren spannungsführender Leitungen

- Beachten Sie: Spannungen über 30 V AC (Wechselstrom) oder 60 V DC (Gleichstrom) sind gefährlich!
- Arbeiten am Niederspannungsnetz (<1000 V AC) dürfen nur mit entsprechender Qualifizierung oder durch einen qualifizierten Elektrotechniker durchgeführt werden und müssen den nationalen/lokalen Bestimmungen für elektrische Anschlüsse entsprechen.

1.2.2 Warnhinweise: Warnung

Warnhinweise des Typs Warnung kennzeichnen eine allgemein gefährliche Situation, die Tod oder schwere Verletzungen zur Folge haben kann.



WARNUNG

Elektrischer Schlag durch Berühren spannungsführender Leitungen

- Schutzerden Sie die Kommunikationssysteme OpenScape Business X3R, X3W, X5R und X5W durch einen separaten Schutzleiter. Verbinden Sie Ihr Kommunikationssystem vor Inbetriebnahme und Anschluss der Telefone und Leitungen ordnungsgemäß mit dem Schutzleiter.
- Schutzerden Sie jede Systembox des Kommunikationssystems OpenScape Business X8 durch einen separaten Schutzleiter. Verbinden Sie Ihr Kommu-

nikationssystem vor Inbetriebnahme und Anschluss der Telefone und Leitungen ordnungsgemäß mit dem Schutzleiter.

- Benutzen Sie Systeme, Geräte und Betriebsmittel nur im einwandfreien Zustand. Die Inbetriebnahme von Geräten mit äußeren Beschädigungen ist verboten.
- Erneuern Sie beschädigte Sicherheitseinrichtungen (Abdeckungen, Aufkleber und Schutzleitungen) sofort.
- Wechseln Sie das Netzkabel sofort aus, wenn es Beschädigungen aufweist.
- Nehmen Sie die Kommunikationssysteme und Server nur über Steckdosen mit angeschlossenem Schutzkontakt in Betrieb.
- Während eines Gewitters sollten Sie Leitungen weder anschließen noch entfernen und Baugruppen weder einbauen noch entfernen.
- Trennen Sie sämtliche Versorgungsstromkreise, wenn die Stromversorgung eines Kommunikationssystems für bestimmte Arbeiten nicht erforderlich ist (zum Beispiel bei Änderungen der Verkabelung). Ziehen Sie sämtliche Netzstecker des Kommunikationssystems und vergewissern Sie sich, dass das Kommunikationssystem nicht von einer zusätzlichen Spannungsquelle (zum Beispiel eine unterbrechungsfreie Stromversorgung) versorgt wird.

  Prüfen Sie vor Beginn jeder Arbeit, ob das Kommunikationssystem spannungsfrei ist. Halten Sie es nie für selbstverständlich, dass mit Ausschalten einer Sicherung oder eines Hauptschalters alle Stromkreise auch zuverlässig unterbrochen sind.
- Rechnen Sie mit Ableitstrom aus dem Telekommunikationsnetz. Trennen Sie alle Telekommunikationsleitungen vom Kommunikationssystem, bevor der vorgeschriebene Schutzleiter vom System getrennt wird.
- Führen Sie Messungen an spannungsführenden Teilen sowie Wartungsarbeiten an Baugruppen und Abdeckungen nur mit der allergrößten Vorsicht aus, solange die Stromversorgung eingeschaltet ist.

  Metallisch beschichtete Oberflächen (zum Beispiel Spiegel) sind stromleitend, bei Berührung besteht die Gefahr eines elektrischen Schlages oder eines Kurzschlusses.

1.2.3 Warnhinweise: Vorsicht

Warnhinweise des Typs Vorsicht kennzeichnen eine gefährliche Situation, die Verletzungen zur Folge habe kann.



VORSICHT

Explosionsgefahr bei unsachgemäßem Austausch von Akkus und Batterien

- Verwenden Sie ausschließlich die zugelassenen Akkus.
- Ersetzen Sie die Lithium-Batterie nur durch identische oder vom Hersteller empfohlene Typen.



VORSICHT

Brandgefahr

- Verwenden Sie nur Kommunikationsleitungen mit einem Leiterdurchmesser von mindestens 0,4 mm (AWG 26) oder größer.
- Hinterlegen Sie keine Unterlagen oder ähnliche brennbare Gegenstände in einem Kommunikationssystem.



VORSICHT

Verletzungsgefahr durch Laserstrahlung

Blicken Sie nicht in den Strahl einer optische Schnittstelle.



VORSICHT

Allgemeine Verletzungs- bzw. Unfallgefahr am Arbeitsplatz

- Installieren Sie nach Test- und Wartungsarbeiten alle Sicherheitseinrichtungen wieder am richtigen Platz und schließen Sie die Deckel und Gehäuse wieder.
- Verlegen Sie Leitungen so, dass sie keine Unfallquelle (Stolpergefahr) bilden und nicht beschädigt werden.
- Stellen Sie sicher, dass bei Arbeiten an einem geöffneten Kommunikationssystem oder Server dieses nie unbeaufsichtigt bleibt.
- Verwenden Sie geeignete Hilfsmittel, um schwere Gegenstände oder Lasten zu heben.
- Prüfen Sie Ihr Werkzeug regelmäßig. Benutzen Sie nur intaktes Werkzeug.
- Tragen Sie bei Arbeiten an den Anlagen keine lose Kleidung und binden Sie längeres Haar immer zurück.
- Tragen Sie keinen Schmuck, metallene Uhrbänder oder zum Beispiel Metallbeschläge und Nieten an Kleidungsstücken.
- Tragen Sie bei entsprechenden Arbeiten immer den erforderlichen Augenschutz.
- Tragen Sie überall dort einen Schutzhelm, wo herabfallende Gegenstände Sie gefährden können.
- Sorgen Sie für gute Beleuchtung am Arbeitsplatz und achten Sie auf Ordnung.

1.2.4 Warnhinweise: Hinweis

Warnhinweise des Typs Hinweis kennzeichnen Situationen, die Sachschäden und/oder Datenverlust zur Folge haben können.

Beachten Sie die folgenden Hinweise, um Sachbeschädigungen und/oder Datenverlust zu vermeiden:

- Prüfen Sie vor der Inbetriebnahme, ob die Nennspannung der Netzspannungsversorgung mit der Nennspannung des Kommunikationssystems oder Servers übereinstimmt (Typenschild).
- Befolgen Sie folgende EGB-Maßnahmen zum Schutz der elektrostatisch gefährdeten Bauelemente:
  - Legen Sie vor allen Arbeiten an Baugruppen und Modulen das Erdungsarmband ordnungsgemäß an.
  - Legen Sie Baugruppen und Module immer auf einer geerdeten, leitfähigen Unterlage ab.
  - Transportieren und versenden Sie Komponenten des Kommunikationssystems (zum Beispiel Baugruppen) nur in geeigneten Verpackungen.

- Verwenden Sie ausschließlich Originalzubehör. Bei Nichtbeachtung können Beschädigungen am Kommunikationssystem auftreten oder Sicherheits- und EMV-Bestimmungen verletzt werden.
- Bei einer plötzlichen Temperaturänderung kann die Luftfeuchtigkeit kondensieren. Wird ein Kommunikationssystem oder Server beispielsweise aus kalter Umgebung in warme Räume gebracht, kann Feuchtigkeit kondensieren. Warten Sie, bis die Temperatur ausgeglichen ist und das Kommunikationssystem oder der Server absolut trocken ist, bevor Sie es in Betrieb nehmen.
- Schließen Sie alle Leitungen nur an den vorgegebenen Anschlusspunkten an.
- Wenn keine Notstromversorgung verfügbar ist oder bei Stromausfall nicht auf analoge Notfalltelefone umgeschaltet werden kann, lassen sich bei einem Ausfall der Stromversorgung keine Notfallanrufe mehr über das Kommunikationssystem tätigen.
- Prüfen Sie vor Beginn einer Wandmontage, ob die Wand eine ausreichende Tragfähigkeit hat. Verwenden Sie immer geeignete Installations- und Befestigungsmittel, um Kommunikationssysteme und Geräte sicher zu montieren.
- Lassen Sie es nicht zu, dass in unmittelbarer Nähe des Kommunikationssystems leicht entflammbare Materialien gelagert werden.

1.2.5 Länderspezifische Sicherheitshinweise

Hier erhalten Sie Informationen über die zu beachtenden Sicherheitshinweise für Montage, Inbetriebnahme und Betrieb des Kommunikationssystems in bestimmten Ländern.

1.2.5.1 Sicherheitshinweise für Australien

Bei der Montage, der Inbetriebnahme und dem Betrieb der Kommunikationssysteme OpenScape Business X und OpenScape Business S sowie des OpenScape Business UC Booster Servers (Application Server) in Australien sind folgende Sicherheitshinweise unbedingt zu beachten:

- Die Kommunikationssysteme OpenScape Business X und OpenScape Business S sowie der OpenScape Business UC Booster Server (Application Server) dürfen nur von autorisiertem Fachpersonal installiert und gewartet werden.
- OpenScape Business Wandsysteme müssen in der Nähe einer Wandsteckdose installiert werden, über die das jeweilige Kommunikationssystem mit Spannung versorgt wird. Die Wandsteckdose muss frei zugänglich sein. Es ist unbedingt sicherzustellen, dass der Erdkontakt der Wandsteckdose intakt ist.
- Die Kommunikationssysteme OpenScape Business X und OpenScape Business S sowie der OpenScape Business UC Booster Server (Application Server) müssen grundsätzlich so konfiguriert werden, dass Notrufnummern (zum Beispiel 000) jederzeit gewählt werden können.

- Bei einem Ausfall der Netzspannungsversorgung können keine Notfallanrufe über das Kommunikationssystem getätigt werden, wenn keine Notstromversorgung verfügbar ist oder bei einem Spannungsausfall nicht auf analoge Notfalltelefone umgeschaltet werden kann (Amtsleitungsumschaltung).
- Wartemusik- und Paging-Geräte müssen über eine von der Australian Communications Authority ACA zugelassene Line Isolation Unit an das Kommunikationssystem angeschlossen werden.

1.2.5.2 Sicherheitshinweise für Brasilien

Bei der Montage, der Inbetriebnahme und dem Betrieb der Kommunikationssysteme OpenScape Business X und OpenScape Business S sowie des OpenScape Business UC Booster Servers (Application Server) in Brasilien sind folgende Sicherheitshinweise unbedingt zu beachten:

- Die Verwendung der Steckdosenleiste mit Überspannungsschutz mit der Sachnummer C39334-Z7052-C33 ist zwingend vorgeschrieben. Der Netzspannungsanschluss der Kommunikationssysteme OpenScape Business X und OpenScape Business S sowie des OpenScape Business UC Booster Servers (Application Server) muss über die Steckdosenleiste mit Überspannungsschutz geführt werden.
- Die Verwendung von abgeschirmten Ethernet-Kabeln für die LAN-/WAN-Schnittstellen/Anschlüsse der Mainboards OCCL, OCCM und OCCMR und der UC Booster Card OCAB (Application Board) ist zwingend vorgeschrieben.

1.2.5.3 Sicherheitshinweise für USA

Bei der Montage, der Inbetriebnahme und dem Betrieb der Kommunikationssysteme OpenScape Business X und OpenScape Business S sowie des OpenScape Business UC Booster Servers (Application Server) in den USA sind folgende Sicherheitshinweise unbedingt zu beachten:

- Netzunterbrechungen und T1-Ausfall
  Bei einer Vernetzung von Kommunikationssystemen über T1 (1,544 MBit/s) muss die Telekommunikationsgesellschaft (Federal Communications Commission FCC) darüber informiert werden, wenn ein Kommunikationssystem aus dem Netz entfernt wird.
  Falls eines der in dieser Dokumentation beschriebenen Kommunikationssysteme der Unify GmbH & Co. KG den Betrieb des öffentlichen Telekommunikationsnetzes stört, ist die Telekommunikationsgesellschaft berechtigt, den Amtszugang vorübergehend zu sperren. Im allgemeinen wird die Telekommunikationsgesellschaft Sie vorab darüber informieren. Falls dies nicht möglich ist, erfolgt die Meldung zum frühsten möglichen Termin. In diesem Zusammenhang werden Sie gleichzeitig darüber informiert, dass Sie eine Beschwerde bei der Telekommunikationsgesellschaft einreichen können.
- Modifikation von Telekommunikationseinrichtungen
  Die Telekommunikationsgesellschaft ist befugt, die eigenen Einrichtungen, Geräte, Betriebsabläufe und Prozesse bei Bedarf anzupassen. Derartige

Modifikationen können gegebenenfalls den Betrieb Ihrer Kommunikationssysteme beeinträchtigen. Im allgemeinen werden Sie vorab benachrichtigt, damit Sie eine Unterbrechung des Telekommunikationsbetriebs vermeiden können.

- Geräte für die Sprachwiedergabe
  Geräte für die Sprachwiedergabe, wie zum Beispiel Wartemusik- und Sprachaufzeichnungsgeräte müssen von der Unify GmbH & Co. KG freigegeben und gemäß den Richtlinien und Bestimmungen der FCC-Vorschriften Teil 68, Unterabschnitt C registriert sein.
  Nicht freigegebene Geräte für die Sprachwiedergabe dürfen nur über Schutzschaltungen angeschlossen werden, die von der Unify GmbH & Co. KG freigegeben und gemäß den Richtlinien und Bestimmungen der FCC-Vorschriften Teil 68, Unterabschnitt C registriert wurden.
- Ringer Equivalence Number REN
  Der Anschlusswert (Ringer Equivalence Number REN) bestimmt, wie viele Geräte gleichzeitig an eine Telefonleitung angeschlossen werden und einen Ruf signalisieren können, wenn die betreffende Rufnummer angewählt wird. In den meisten, jedoch nicht in allen Bereichen, dürfen maximal fünf Geräte an eine Leitung angeschlossen werden (REN = 5). Wenden Sie sich gegebenenfalls an Ihre lokale Telekommunikationsgesellschaft, um festzustellen, wie viele RENs in Ihrem Rufbereich unterstützt werden.
- Neue Ortsnetz- und Amtskennzahlen
  Die Leitweglenkung (Least Cost Routing LCR) ist so zu konfigurieren, dass Änderungen von Ortsnetz- und Amtskennzahlen automatisch erkannt und berücksichtigt werden können. Ansonsten können nach Kennzahländerungen diese nicht für Anrufe genutzt werden.
- Kompatibilität mit Hörhilfen
  Notfalltelefone und öffentliche Telefone (zum Beispiel Telefone in Eingangshallen, Krankenhauszimmern, Aufzügen und Hotelzimmern) müssen mit Handapparaten ausgestattet sein, die den Einsatz magnetisch gekoppelter Hörhilfen gewährleisten. Bei Bedarf müssen für hörgeschädigte Personen, die sich nicht in öffentlichen Bereichen aufhalten, geeignete Handapparate bereitgestellt werden.
  Alle nach dem 16. August 1989 hergestellten digitalen Telefone der Unify GmbH & Co. KG sind kompatibel mit Hörhilfen und erfüllen die Anforderungen gemäß den FCC-Vorschriften, Teil 68, Abschnitt 68.316.
- Programmierte Wählfunktionen
  Wenn Sie Notrufnummern programmieren oder über ein Produkt der Unify GmbH & Co. KG mit programmierten Wählfunktionen eine Testverbindung zu einer Notrufnummer herstellen, müssen Sie die Verbindung halten und dem Einsatzleiter kurz den Grund Ihres Anrufs erklären, bevor Sie auflegen. Diese Maßnahmen sollten zu verkehrsarmen Zeiten durchgeführt werden, beispielsweise am frühen Morgen oder am späten Abend.
- Anschaltung von außenliegenden Nebenstellen
  Kunden, die die Anschaltung von außenliegenden Nebenstellen (Off-Premises Station OPS) wünschen, müssen die Telekommunikationsgesellschaft darüber informieren, für welche OPS-Klasse die betreffenden Geräte registriert sind und welcher Verbindungstyp gewünscht wird.

- Überwachung der Rufannahme bei Durchwahl
  Kunden, die eines der in dieser Dokumentation beschriebenen Kommunikationssysteme der Unify GmbH & Co. KG ohne ordnungsgemäße Rufannahme-Überwachung betreiben, verstoßen gegen Teil 68 der FCC-Vorschriften.
  Die in dieser Dokumentation beschriebenen Kommunikationssysteme der Unify GmbH & Co. KG unterstützen ordnungsgemäße Rückmeldungen an das öffentliche Telekommunikationsnetz, wenn Durchwahlanrufe
  - von dem gerufenen Teilnehmer angenommen werden.
  - von einer Vermittlungsperson angenommen werden.
  - an eine kundenseitig verwaltete Ansage weitergeleitet werden.

  Ferner unterstützen die in dieser Dokumentation beschriebenen Kommunikationssysteme der Unify GmbH & Co. KG ordnungsgemäße Rückmeldungen für Durchwahlanrufe, die an das öffentliche Telekommunikationsnetz weitergeleitet werden. Zulässige Ausnahmen:
  - Ein Anruf wird nicht angenommen.
  - Es wird besetzt signalisiert.
  - Es wird gassenbesetzt (Reorder Tone) signalisiert.
- Voraussetzungen für den gleichberechtigten Zugriff
  Für Bereiche mit erhöhtem Verkehrsaufkommen (zum Beispiel Hotels, Krankenhäuser, Flughäfen, Schulen) müssen den Teilnehmern gleichberechtigte Zugangscodes für die gewünschten Provider zur Verfügung gestellt werden. Die aktuellen Codes für den gleichberechtigten Zugang (Carrier Access Codes CAC) lauten 10xxx und 101xxxx, sowie 800/888 und 950, wobei xxx oder xxxx für den jeweilige Provider-Code steht.
  Um eine Verbindung über einen bestimmten Provider herzustellen, muss der Teilnehmer vor der Rufnummer des gewünschten Gesprächspartners zunächst einen Provider-spezifischen Zugangscode eingeben. Der gleichberechtigte Zugang ist auch über die Codes 800/888 oder 950 des gewünschten Providers möglich.
  Über gleichberechtigte Zugangscodes unterstützen die in dieser Dokumentation beschriebenen Kommunikationssysteme der Unify GmbH & Co. KG den Zugang zu Interstate Providern.
  Modifikationen dieser Funktionalität stellen eine Verletzung des Telephone Operator Consumer Services Improvement Act von 1990 sowie Teil 68 der FCC-Vorschriften dar.

1.2.5.4 Sicherheitshinweise für Kanada



GEFAHR

Elektrischer Schlag durch Berühren spannungsführender Leitungen

Arbeiten am Niederspannungsnetz (<1000 V AC) dürfen nur mit entsprechender Qualifizierung oder durch einen qualifizierten Elektrotechniker durchgeführt

werden und müssen den nationalen/lokalen Bestimmungen für elektrische Anschlüsse entsprechen.

Bei der Montage, der Inbetriebnahme und dem Betrieb der Kommunikationssysteme OpenScape Business X und OpenScape Business S sowie des OpenScape Business UC Booster Servers (Application Server) in Kanada sind folgende Sicherheitshinweise unbedingt zu beachten:

- Ringer Equivalence Number REN
  Der Anschlusswert (Ringer Equivalence Number REN) bestimmt, wie viele Geräte gleichzeitig an eine Telefonleitung angeschlossen werden können. Der Schnittstellenabschluss kann eine beliebige Gerätekombination umfassen, vorausgesetzt, die REN-Anzahl aller Geräte ist kleiner oder gleich fünf.
- Einschränkungen für den Anschluss von Geräten
  Zertifizierte Geräte sind mit einem Industry-Canada-Aufkleber gekennzeichnet. Diese Zertifizierung besagt, dass die Geräte bestimmte Anforderungen im Hinblick auf den Schutz, den Betrieb und die Sicherheit von Telekommunikationsnetzen erfüllen. Die Anforderungen sind in den Terminal Equipment Technical Requirements dokumentiert. Industry Canada gibt keine Zusicherungen, dass zertifizierte Geräte jederzeit zur Kundenzufriedenheit funktionieren.
  Vor Installation der in dieser Dokumentation beschriebenen Geräten und Komponenten sollte der Benutzer sicherstellen, dass eine Anschaltung an Einrichtungen der lokalen Telekommunikationsgesellschaft gestattet ist. Außerdem ist bei Installation der Kommunikationssysteme und Server darauf zu achten, dass ein geeignetes Anschlussverfahren gewählt wird. Der Kunde sollte darauf hingewiesen werden, dass auch bei Einhaltung aller genannten Vorgaben in bestimmten Situationen Leistungseinbußen auftreten können.
  Reparaturen an zertifizierten Geräten sollten von einem Servicetechniker des Herstellers oder Lieferanten koordiniert werden. Benutzerseitig durchgeführte Reparaturen oder Modifikationen an den in dieser Dokumentation beschriebenen Geräten und Komponenten oder Gerätefehlfunktionen können die Telekommunikationsgesellschaft dazu berechtigen, den Benutzer aufzufordern, die betreffenden Geräte zu deinstallieren.
  Zur eigenen Sicherheit sollte der Benutzer sicherstellen, dass die elektrischen Erdungsverbindungen von Stromversorgung, Telefonleitungen und metallischem Wasserleitungssystem (sofern vorhanden) miteinander verbunden sind. Insbesondere in ländlichen Gebieten kann diese Vorsichtsmaßnahme besonders wichtig sein.

1.3 Wichtige Hinweise

Die wichtigen Hinweise informieren Sie über das Verhalten in Notfällen, die sachgemäße Entsorgung und das sachgemäße Recycling und den bestimmungsgemäßen Gebrauch und die Betriebsbedingungen der Kommunikationssysteme und Server. Darüber hinaus erhalten Sie Angaben über die Normen und Richtlinien bezüglich der Installation, die Funkstöreigenschaften der Kommunikationssysteme und über Datenschutz und Datensicherheit.

Verwandte Themen

- Sicherheits- und Warnhinweise

1.3.1 Verhalten in Notfällen

Hier erhalten Sie Informationen über die Maßnahmen, die bei einem Notfall zu ergreifen sind.

Vorgehensweise bei Unfällen

- Gehen Sie bei Unfällen stets überlegt und mit Ruhe vor.
- Schalten Sie immer zuerst die Stromversorgung aus, bevor Sie ein Unfallopfer berühren.
- Falls Sie die Stromversorgung auf Anhieb nicht ausschalten können, berühren Sie das Opfer nur mit nicht leitenden Materialien (z. B. Besenstiel aus Holz), und versuchen Sie als erstes, es von der Stromquelle zu isolieren.

Erste Hilfe Maßnahmen

- Die Grundsätze der ersten Hilfe bei Stromschlägen müssen Ihnen vertraut sein. Dringend notwendig in solchen Notfällen sind Grundkenntnisse der verschiedenen Wiederbelebungsmaßnahmen für den Fall eines Atem- oder Herzstillstands sowie die ersten Maßnahmen bei Verbrennungen.
- Führen Sie bei Atemstillstand sofort eine Atemspende (Mund-zu-Mund oder Mund-zu-Nase) durch.
- Falls Sie über eine entsprechende Ausbildung verfügen, führen Sie bei Herzstillstand sofort eine Herzdruckmassage durch.

Notruf

Rufen Sie unverzüglich einen Krankenwagen oder den Notarzt. Geben Sie den Notruf in folgender Reihenfolge durch:

- Wo geschah was?
- Was geschah?
- Wie viele Verletzte?
- Welche Art von Verletzungen?
- Warten auf Rückfragen.

Meldung von Unfällen

- Melden Sie umgehend alle Unfälle, “Beinahe-Unfälle" und potentielle Gefahrenquellen an Ihren Vorgesetzten.
- Melden Sie jeden elektrischen Stromschlag, auch wenn er nur schwach war.

1.3.2 Bestimmungsgemäßer Gebrauch

Die Kommunikationssysteme und Server dürfen nur für die in dieser Dokumentation beschriebenen Einsatzmöglichkeiten und nur in Verbindung mit den von Unify GmbH & Co. KG empfohlenen und zugelassenen Zusatzgeräten und -komponenten verwendet werden.

Der bestimmungsgemäße Gebrauch der Kommunikationssysteme und Server setzt sachgemäßen Transport, sachgemäße Lagerung, Montage und Inbetriebnahme sowie sorgfältige Bedienung und Instandhaltung voraus.

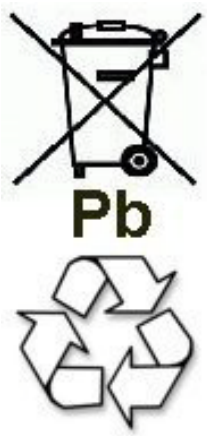
INFO: Reinigen Sie das Gehäuse von Kommunikationssystem und Server nur mit einem weichen, leicht feuchten Tuch. Benutzen Sie keine scharfen Reiniger oder Scheuerschwämme.

1.3.3 Sachgemäße Entsorgung und Recycling

Beachten Sie die Informationen über die sachgemäße Entsorgung und das sachgemäße Recycling von Elektro- und Elektronikgeräten und von Altbatterien und Akkus.



Alle Elektro- und Elektronikgeräte sind getrennt vom allgemeinen Hausmüll über dafür staatlich vorgesehene Stellen zu entsorgen. Die sachgemäße Entsorgung und die getrennte Sammlung von Altgeräten dient der Vorbeugung von potentiellen Umwelt- und Gesundheitsschäden. Sie sind eine Voraussetzung für die Wiederverwendung und das Recycling gebrauchter Elektro- und Elektronikgeräte. Ausführliche Informationen zur Entsorgung Ihrer Altgeräte erhalten Sie bei Ihrer Kommune, Ihrem Müllentsorgungsdienst, dem Fachhändler bei dem Sie das Produkt erworben haben oder Ihrem Vertriebsansprechpartner. Diese Aussagen sind nur gültig für Geräte, die in den Ländern der Europäischen Union installiert und verkauft werden und die der Europäischen Richtlinie 2002/96/EC unterliegen. In Ländern außerhalb der Europäischen Union können davon abweichende Bestimmungen für die Entsorgung von Elektro- und Elektronikgeräten gelten.



Altbatterien oder Akkus mit diesem Zeichen sind verwertbares Wirtschaftsgut und müssen dem Recyclingprozess zugeführt werden. Altbatterien oder Akkus, die nicht dem Recyclingprozess zugeführt werden, sind unter Beachtung aller Vorschriften als Sondermüll zu entsorgen.

1.3.4 Normen und Richtlinien bezüglich der Installation

Beachten Sie die Informationen, welche Vorgaben beim Anschluss der Kommunikationssysteme und Server an den Versorgungsstromkreis und bei der geschirmten Verkabelung für LAN- und WAN-Anschlüsse einzuhalten sind.

1.3.4.1 Anschluss von OpenScape Business X an den Versorgungsstromkreis

Die Kommunikationssysteme OpenScape Business X sind zum Anschluss an TN-S-Energieversorgungssysteme freigegeben. Ebenfalls erlaubt ist der Anschluss an ein TN-C-S-Energieversorgungssystem, bei dem der PEN-Leiter in jeweils einen Schutz- und Neutralleiter aufgeteilt ist. TN-S und TN-C-S gemäß Definition der Norm IEC 364-3.

Sind Arbeiten am Niederspannungsnetz erforderlich, müssen diese von einem qualifizierten Elektrotechniker durchgeführt werden. Diese Installationstätigkeiten zum Anschluss der Kommunikationssysteme müssen unter Beachtung der IEC 60364-1 und der IEC 60364-4-41 oder entsprechender gesetzlicher Normen bzw. nationaler Vorschriften erfolgen.

1.3.4.2 Anschluss von OpenScape Business S und OpenScape Business UC Booster Server an den Versorgungsstromkreis

Angaben zum Anschluss von OpenScape Business S und OpenScape Business UC Booster Server (Application Server) an den Versorgungsstromkreis entnehmen Sie bitte den Herstellerunterlagen des Server-PCs und der weiteren Komponenten.

Sind Arbeiten am Niederspannungsnetz erforderlich, müssen diese von einem qualifizierten Elektrotechniker durchgeführt werden. Diese Installationstätigkeiten zum Anschluss von OpenScape Business S und OpenScape Business UC Booster Server müssen unter Beachtung der IEC 60364-1 und der IEC 60364-4-

41 oder entsprechender gesetzlicher Normen bzw. nationaler Vorschriften (zum Beispiel in den USA und in Kanada) erfolgen.

1.3.4.3 Geschirmte Verkabelung für LAN- und WAN-Anschlüsse von OpenScape Business X

Die Einhaltung der CE-Anforderungen bezüglich elektromagnetischer Verträglichkeit der Kommunikationssysteme OpenScape Business X und deren LAN- und WAN-Anschlüsse setzt folgende Bedingung voraus:

- Der Betrieb der Kommunikationssysteme ist nur mit geschirmter Anschlussverkabelung erlaubt. Das bedeutet zwischen den geschirmten LAN- und WAN-Anschlussbuchsen der Kommunikationssysteme und dem Anschluss an die Gebäudeinstallation oder dem Anschluss an externe aktive Komponenten ist ein geschirmtes Kategorie-5-Kabel (CAT.5-Kabel) mit einer Länge von mindestens 3 m zu verwenden. An dem der Gebäudeinstallation oder der externen aktiven Komponente zugewandten Kabelende ist der Kabelschirm zu erden (Verbindung zum Gebäudepotentialausgleich).
- Bei kürzeren Verbindungen mit einer externen aktiven Komponente (LAN-Switch oder ähnliches) ist ebenfalls ein geschirmtes Kategorie-5-Kabel (CAT.5-Kabel) zu verwenden. Jedoch muss die aktive Komponente einen entsprechend geschirmten LAN-Anschluss aufweisen, dessen Schirmanschluss geerdet ist (Verbindung zum Gebäudepotentialausgleich).
- Die Schirmeigenschaften der Verkabelungskomponenten sollen die Anforderungen der Europäischen Norm EN 50173-1[*)] "Anwendungsneutrale Kommunikationskabelanlagen" (und der dort genannten Verweise) mindestens erfüllen.[***)]
- Gebäudeinstallationen, die mit durchgängig geschirmter symmetrischer Kupfer-Verkabelung gemäß den Klasse D-Anforderungen[**)] der EN 50173-1 ausgestattet sind, erfüllen die oben genannten Bedingung.[***)]

*) Die europäische Norm EN 50173-1 ist aus dem globalen Standard ISO/IEC 11801 abgeleitet.

**) Klasse D wird unter anderem erreicht, wenn Komponenten (Kabel, Anschlussdosen, Anschlusskabel, etc.) der Kategorie 5 (CAT.5) installiert sind.

***) Im nordamerikanischen Markt ist überwiegend UTP-Verkabelung (US-Norm EIA/TIA 568 A) installiert, daher gilt dort für die LAN- und WAN-Anschlüsse der Kommunikationssysteme: Der Betrieb der Systeme ist nur mit geschirmter Anschlussverkabelung erlaubt. Das bedeutet zwischen den geschirmten LAN- und WAN-Anschlussbuchsen der Kommunikationssysteme und dem Anschluss an die Gebäudeinstallation oder dem Anschluss an externe aktive Komponenten ist ein geschirmtes Kategorie-5-Kabel (CAT.5-Kabel) mit einer Länge von mindestens 3 m zu verwenden. An dem der Gebäudeinstallation oder der externen aktiven Komponente zugewandten Kabelende ist der Kabelschirm zu erden (Verbindung zum Gebäudepotentialausgleich).

1.3.4.4 Brandschutzanforderungen

Brandschutzanforderungen sind in den Bauordnungen länderspezifisch geregelt. Die jeweils gültigen Vorschriften sind zu beachten.

Um die gesetzlich geforderten Brandschutz- und EMV-Anforderungen zu gewährleisten, dürfen die Kommunikationssysteme OpenScape Business X nur geschlossen betrieben werden. Ein Öffnen ist nur kurzzeitig zu Montage- und Wartungszwecken gestattet.

Die OpenScape-Business-Systemkabel entsprechen bezüglich des Brennverhaltens den Anforderungen des internationalen Standards IEC 60332-1. Die folgenden Standards enthalten gleichwertige Anforderungen bezüglich des Brennverhaltens von Kabeln:

IEC 60332-1 Hinweis: IEC 60332-1 entspricht der Prüfart UL VW-1	EN 50265-1 mit EN 50265-2-1 Hinweis: EN 50265-1 und -2-1 -ersetzen HD 405.1	VDE 0482 Teile 265-1 mit VDE 0482 Teile 265-2-1 Hinweis: VDE 0482 Teile 265-1 und -2-1 ersetzen VDE 0472, Teil 804, Prüfart B

Ob der Standard IEC 60332-1 den jeweiligen Bauordnungen und eventuell darüber hinausreichenden Vorschriften genügt, ist durch den verantwortlichen Bereich in Projektierung und Service zu prüfen.

1.3.4.5 Blitzschutzanforderungen

Der Schutz der Kommunikationssysteme gegen energiereiche Überspannungen erfordert eine niederohmige Erdanbindung gemäß den Angaben in der *Servicedokumentation OpenScape Business V1*.

HINWEIS: Nach der Schutzerdung eines Kommunikationssystems ist die niederohmige Erdanbindung des Systems über den Schutzleiter des Netzspannungsversorgungskreises und die niederohmige Anbindung des zusätzlichen, permanent angeschlossenen Schutzerdungsleiters zur Potentialausgleichsschiene des Gebäudes zu prüfen.

HINWEIS: Brandgefahr durch Überspannung

Telekommunikationsleitungen über 500 m Länge oder Telekommunikationsleitungen, die das Gebäude verlassen müssen über einen zusätzlichen externen Blitzschutz geführt werden.

Ein solcher Blitzschutz wird als zusätzlicher Primärschutz bezeichnet. Der zusätzliche Primärschutz wird durch den fachgerechten Einbau von ÜSAGs (Überspannungsableiter, gasgefüllt) im Hauptverteiler, im Patch-Panel oder am Eintrittspunkt der Leitung in das Gebäude gewährleistet. Dazu muss ein ÜSAG mit

230 V Nennspannung von jeder zu schützenden Ader gegen Erde geschaltet werden.

Ohne diesen zusätzlichen Primärschutz kann es bei einer Blitzbeeinflussung zu einer Zerstörung von Baugruppen kommen. Dies kann zum Ausfall des gesamten Kommunikationssystems und zur Überhitzung von Bauelementen führen (Brandgefahr).

1.3.4.6 Kennzeichnungen für OpenScape Business X



Die Konformität des Gerätes zu der EU-Richtlinie 1999/5/EG wird durch das CE-Kennzeichen bestätigt.

1.3.5 Hinweise zu Störaussendung und Funkstörung von OpenScape Business X

Die Kommunikationssysteme OpenScape Business X sind Einrichtungen der Klasse B gemäß EN 55022.

1.3.6 Datenschutz und Datensicherheit

Beachten Sie die Informationen zur Gewährleistung des Datenschutzes und der Datensicherheit.

Bei den in dieser Dokumentation beschriebenen Kommunikationssystemen und Servern werden unter anderem personenbezogene Daten verarbeitet und genutzt, zum Beispiel bei der Gebührenerfassung, den Displayanzeigen, der Kundendatenerfassung.

In Deutschland gelten für die Verarbeitung und Nutzung solcher personenbezogenen Daten unter anderem die Bestimmungen des Bundesdatenschutzgesetzes (BDSG). Für andere Länder beachten Sie bitte die jeweiligen entsprechenden Landesgesetze.

Datenschutz hat die Aufgabe, den einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

Ferner hat Datenschutz die Aufgabe, durch den Schutz der Daten vor Missbrauch in ihren Verarbeitungsphasen der Beeinträchtigung fremder und eigener schutzwürdiger Belange zu begegnen.

INFO: Der Kunde ist dafür verantwortlich, dass Kommunikationssysteme und Server in Übereinstimmung mit dem jeweils gültigen Datenschutz-, Arbeits- und Arbeitsschutzrecht installiert, betrieben und gewartet werden.

Mitarbeiter der Unify GmbH & Co. KG sind durch die Arbeitsordnung zur Wahrung von Geschäfts- und Datengeheimnissen verpflichtet.

Um die gesetzlichen Bestimmungen beim Service – ob beim “Service vor Ort" oder bei “Remote Services" – konsequent einzuhalten, sollten Sie folgende Regeln unbedingt befolgen. Sie wahren damit nicht nur die Interessen Ihrer und unserer Kunden, sondern vermeiden dadurch auch persönliche Konsequenzen.

Tragen Sie durch problembewusstes Handeln mit zur Gewährleistung des Datenschutzes und der Datensicherheit bei:

- Achten Sie darauf, dass nur berechtigte Personen Zugriff auf Kundendaten haben.
- Nutzen Sie alle Möglichkeiten der Passwortvergabe konsequent aus; geben Sie keinem Unberechtigten Kenntnis der Passwörter, zum Beispiel per Notizzettel.
- Achten Sie mit darauf, dass kein Unberechtigter in irgendeiner Weise Kundendaten verarbeiten (speichern, verändern, übermitteln, sperren, löschen) oder nutzen kann.
- Verhindern Sie, dass Unbefugte Zugriff auf Datenträger haben, zum Beispiel auf Sicherungs-CDs-/DVDs oder Protokollausdrucke. Das gilt sowohl für den Serviceeinsatz, als auch für Lagerung und Transport.
- Sorgen Sie dafür, dass nicht mehr benötigte Datenträger vollständig vernichtet werden. Vergewissern Sie sich, dass keine Papiere allgemein zugänglich zurückbleiben.
- Arbeiten Sie mit Ihren Ansprechpartnern beim Kunden zusammen: Das schafft Vertrauen und entlastet Sie selbst.

1.3.7 Technische Vorschriften und Konformität von OpenScape Business X

Hier erhalten Sie Informationen über die Erfüllung festgelegter Forderungen (Konformität) durch die Kommunikationssysteme OpenScape Business X.

1.3.7.1 CE-Konformität

Basis der CE-Kennzeichnung ist die R&TTE-Directive 99/5/EEC.

	Normenreferenz
Safety	EN 60950-1
Electromagnetic Compatibility EMC	EN55022 (EMC Emission) EN55024 (EMC Immunity Residential)
Digital Enhanced Cordless Telecommunications DECT	ETS 300 329 (DECT Emission/Immunity) TBR 06, ETS 301489-1/6 (DECT Air Interface)

1.3.7.2 Konformität mit US- und kanadischen Normen

	Normenreferenz
Safety USA	UL 60950-1
Safety Kanada	CSA C22.2 No. 60950-1-03
EMC Emission	FCC Part 15 Subpart J Class B

FCC-Registrierungsnummer und Anschlusswert

Auf der Gehäuserückseite der Kommunikationssysteme befindet sich ein Aufkleber mit der FCC-Registrierungsnummer, dem Anschlusswert (Ringer Equivalence Number REN) sowie weiteren Informationen. Diese Informationen können auf Anforderung an die Telekommunikationsgesellschaft weitergegeben werden.

1.3.7.3 Konformität mit internationalen Normen

	Normenreferenz
Safety	IEC 60950-1

1.3.8 Betriebsbedingungen

Beachten Sie die klimatischen und mechanischen Bedingungen für den Betrieb der Kommunikationssysteme OpenScape Business X und OpenScape Business S sowie des OpenScape Business UC Booster Servers (Application Server).

1.3.8.1 Betriebsbedingungen OpenScape Business X

Angegeben sind die klimatischen und mechanischen Bedingungen für den Betrieb der Kommunikationssysteme OpenScape Business X.

Klimatische Betriebsbedingungen

Grenzbetriebsbereich:

- Raumtemperatur: + 5 bis + 40 °C (41 bis 104 °F)
- absolute Luftfeuchte: 1 bis 25 g H_2O/m^3
- relative Luftfeuchte: 5 bis 80%

Die Entlüftung der Kommunikationssysteme erfolgt durch Konvektion. Zwangsentlüftung ist bei OpenScape Business X5W erforderlich, wenn mehr als 32 a/b-Schnittstellen vorhanden sind.

HINWEIS: Schäden durch lokale Temperaturerhöhungen

Vermeiden Sie direkte Sonneneinstrahlung oder Wärmeeinwirkung durch Heizkörper auf die Kommunikationssysteme.

HINWEIS: Schäden durch Kondensation von Luftfeuchtigkeit

Vermeiden Sie unter allen Umständen vor und während des Betriebs die Kondensation von Luftfeuchtigkeit auf oder in den Kommunikationssystemen.

Ein Kommunikationssystem muss absolut trocken sein, bevor Sie es in Betrieb nehmen.

Mechanische Betriebsbedingungen

Die Kommunikationssysteme sind grundsätzlich für stationären Einsatz entwickelt worden.

1.3.8.2 Betriebsbedingungen OpenScape Business S und OpenScape Business UC Booster Server

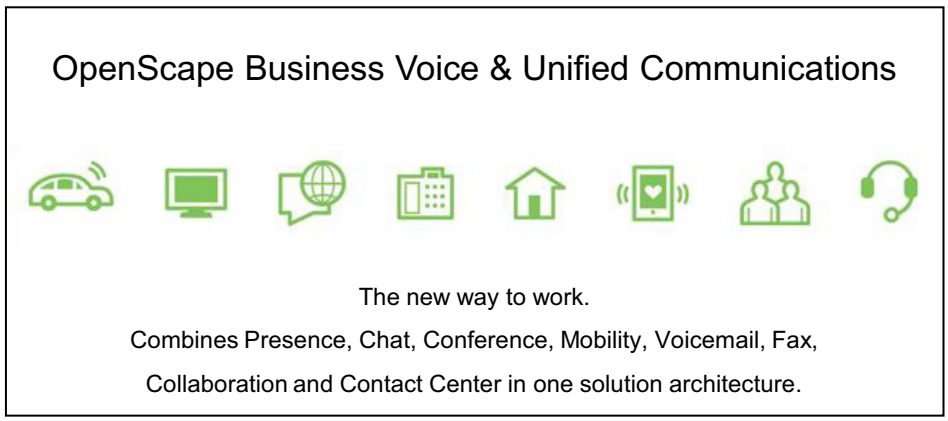
Angaben zu den klimatischen und mechanischen Bedingungen für den Betrieb von OpenScape Business S und OpenScape Business UC Booster Server (Application Server) entnehmen Sie bitte den Herstellerunterlagen der Server-PCs und der weiteren Komponenten.

2 Systemüberblick

OpenScape Business bietet kleinen und mittleren Unternehmen die Antwort auf deren individuelle und vielseitige Kommunikationsanforderungen, vereint in einer flexiblen und skalierbaren Lösung. Die OpenScape Business Lösungsarchitektur ermöglicht den Einsatz unabhängig von der vorhandenen Telefonie-Infrastruktur, egal ob klassische Telefonie, IP oder DECT. Von leistungsstarker Telefonie bis zur umfassenden Unified Communications (UC) Komplettlösung liefert OpenScape Business Unternehmen mit bis zu 500 Teilnehmern, bzw. 1000 Teilnehmern in einem Netzwerk, immer die richtige Lösung.

Flexibel, skalierbar und leistungsstark

OpenScape Business führt das Beste aus HiPath 3000 und OpenScape Office in einer neuen Lösungsplattform zusammen.



2.1 Highlights

OpenScape Business ist die All-In-One-Lösung für kleine und mittlere Unternehmen und bietet folgende Highlights.

Highlights

- integrierte Sprachdienste, Präsenzmanagement (Anwesenheitsstatus), Drag&Drop-Konferenz, visuelle Voicemail (Sprachboxen), AutoAttendant, Multimedia Contact Center, IM (Instant Messaging, Sofortnachrichten), Mobility, Verzeichniszugriff mit Datenbank-Anbindung, Fax, Integration in Geschäftsprozesse und vieles mehr
- individuell auf den Arbeitsplatz und die Arbeitsweise abgestimmte UC Clients
- Oberflächen-Integration von OpenScape Web Collaboration
- für Kunden mit einem Standort oder als netzweite Lösung mit mehreren Standorten
- OpenScape Business bietet eine einheitliche Lösungsarchitektur.
- in Abhängigkeit von der vorhandenen Infrastruktur sind verschiedene OpenScape Business Modelle für unterschiedliche Ausbaugrößen verfügbar

oder alternativ besteht die Möglichkeit die OpenScape Business Software auf einem Standard-Server zu betreiben (Softswitch) - selbstverständlich auch in voll virtualisierten Umgebungen

- unabhängig vom Modell werden immer 500 Teilnehmer unterstützt (Summe aus IP-, analogen und digitalen Teilnehmern)
- optimiertes Hardwarekonzept: VoIP- und Data-Komponenten sind bereits auf dem Mainboard integriert. UC für bis zu 50 Benutzer ist ebenfalls auf dem Mainboard vorgeleistet (UC Smart), erweiterbar für mehr Benutzer und weitere UC-Funktionalität (UC Suite) durch eine UC Booster Card (für bis zu 150 Benutzer) oder einen UC Booster Server (für bis zu 500 Benutzer).
- UC-Software und Hardware inkl. Drag&Drop-Konferenz und Multimedia Contact Center für alle Modelle
- für die vielseitigen und heterogenen Anforderungen sind alle Kommunikationsschnittstellen bereits vorhanden: IP, digital, analog und DECT sowie alle gängigen Amtschnittstellen für die Sprachkommunikation

2.2 Unified Communications

Unified Communications (UC) ist eine Technologie zur Verbesserung der Kommunikation in Unternehmen und integriert verschiedene Kommunikationsmedien in einer einheitlichen Anwendungsumgebung. Unified Communications vereinfacht die Geschäftsprozesse im Unternehmen durch ein durchgängiges Präsenzmanagement (z. B. werden Anrufe automatisch zum Mobiltelefon umgeleitet, wenn sie außer Haus sind). Auch die Bereitstellung von Einwahlkonferenzen, persönlicher Voicemail (Sprachbox), persönlicher Faxbox, Instant Messaging (IM), Einsatz des Mobiltelefons als Nebenstelle des Kommunikationssystems, Contact Center, Video und Web Collaboration sind in dieser einheitlichen Lösung vereint.

Mit dem flexiblen Unified-Communication-Ansatz der OpenScape Business werden, je nach Anforderung an den Arbeitsplatz und der vorhandenen Infrastruktur, verschiedene UC-Lösungen angeboten. Bei der UC-Lösung wählen Sie zwischen UC Smart und UC Suite (UC Smart und UC Suite können nicht parallel genutzt werden).

Die bereits auf dem UC-Mainboard der OpenScape Business X integrierte UC-Smart-Lösung kann jederzeit über Upgrade-Lizenz auf die erweiterte UC-Suite-Lösung migriert werden. Je nach Anzahl der UC-Teilnehmer muss dann OpenScape Business nur noch durch die PlugIn-Baugruppe (UC Booster Card) oder mit dem UC Booster Server (externer Server) erweitert werden. Als reiner Softswitch steht die OpenScape Business S als Server-Lösung mit UC Suite zur Verfügung.

2.2.1 UC-Funktionen (Überblick)

Abhängig von der gewählten UC-Lösung (UC Smart oder UC Suite) stehen Ihnen unterschiedliche UC-Funktionen zur Verfügung.

Die folgenden Tabellen sollen Ihnen helfen, die vor Sie geeignete UC-Lösung auszuwählen. Detaillierte funktionale Randbedingungen finden Sie in den entsprechenden Kapiteln (UC Smart, UC Suite, Attendants) der Leistungsmerkmalbeschreibung bzw. Administratordokumentation.

UC-Funktion	UC Smart			UC Suite			Anmerkung
	myPortal Smart	**myPortal for Mobile**	**myPortal to go**	**myPortal for Desktop/Outlook**	**myPortal for Mobile**	**myPortal to go**	
Anwesenheitsstatus							
Anwesenheitsstatus (Präsenz-Management)	x	x	x	x	x	x	
Änderung des Anwesenheitsstatus über Client	x	x	x	x	x	x	
Änderung des Anwesenheitsstatus über TUI	-	-	-	x	-	-	
Statusbezogene Anrufumleitung	x	x	x	x	über myPortal definierte Ziele	über myPortal definierte Ziele	Bei UC Smart kann eine beliebige Nummer als Ziel ausgewählt werden. Bei UC Suite kann nur eine Nummer aus der Vorauswahl ausgewählt werden
Statusanzeige in Favoriten	x	x	x	x	x	x	
Statusanzeige in Verzeichnissen	x	x	x	x	x	x	
Statusanzeige im Journal	-	-	-	x	-	-	
CallMe aktivieren	-	-	-	x	x	x	
Kalender-Integration (Outlook)	-	-	-	x	-	-	
Kalender-Integration (iCal) (nur myPortal for Desktop)	-	-	-	x	-	-	
Favoriten							
Anzeige des Anrufstatus	x	x	x	x	x	x	
Anlegen von Gruppen	x	-	x	x	-	-	
Kompakte Anzeige der Favoriten	x	-	-	x	-	-	

UC-Funktion	UC Smart			UC Suite			Anmerkung
	myPortal Smart	myPortal for Mobile	myPortal to go	myPortal for Desktop/Outlook	myPortal for Mobile	myPortal to go	
Verzeichnisse							
Persönliches Verzeichnis	x	x	x	x	x	x	
Internes Verzeichnis	x	x	x	x	x	x	
Externes Verzeichnis	-	-	-	x	x	x	
Suche in Verzeichnissen	x	x	x	x	x	x	Im myPortal Smart auch Schnellsuche
Zugriff auf im System definierte Kurzwahlziele (KWZ)	x	x	x	-	x	x	
Import / Verwalten persönlicher Kontakte (CSV/XML)	x	-	-	x	-	-	
Zugriff auf Outlook-Kontakte	x	-	-	x	-	-	
Import von persönlichen Kontakten (Mac OS) (myPortal for Desktop)	-	-	-	x	-	-	
Integration externer Verzeichnisserver über LDAP	-	-	-	x	-	-	
Journal							
Alle Anrufe	x	x	x	x	x	x	
Offene Anrufe	-	-	-	x	-	-	
Entgangene Anrufe	x	x	x	x	x	x	
Angenommene Anrufe	x	x	x	x	x	x	
Geplante Anrufe	-	-	-	x	-	-	
Sprachnachrichten	-	-	x	x	-	x	
Fax-Journal	-	-	-	x	-	-	
Anrufe							
Manuelle Wahl	x	x	x	x	x	x	
Desktop-Wahl (Click to Call)	x	-	-	x	-	-	
Weiterleiten	x	x	x	x	x	x	
Halten	x	x	x	x	x	x	

UC-Funktion	UC Smart			UC Suite			Anmerkung
	myPortal Smart	**myPortal for Mobile**	**myPortal to go**	**myPortal for Desktop/Outlook**	**myPortal for Mobile**	**myPortal to go**	
Aufzeichnen von Anrufen (Voice Recording)	-	-	-	x	-	-	
E-Mail senden	x	-	x	x	-	x	
SMS senden	-	x	x	-	x	x	
Chat starten	x	-	-	x	-	-	
Popups	x	-	-	x	-	-	
Konferenzen							
AdHoc-Konferenz	x	x	x	x	x	x	
geplante, permanente und offene Konferenzen (Drag&Drop-Konferenz)	-	-	-	x	-	-	
Web Collaboration-Einbindung	-	-	-	x			
Sprach- und Faxnachrichten							
Sprachbox (Visuelle Voicemail)	x	x	x	x	x	x	Voicemail-Funktionalität für Teilnehmer (IP, TDM)
Abhören über Telefon	x	x	x	x	x	x	
Abhören über PC-Soundkarte	-	-	-	x	-	-	
Sprachnachricht als E-Mail senden	x	-	x	x	-	-	
Fax	-	-	-	x	-	-	
Instant Messaging							
Instant Messaging (Chat)	x	-	-	x	-	-	

myPortal to go erlaubt den Zugriff auch auf die lokalen Smartphone Kontakte.

Contact Center

UC-Funktion	UC Smart	UC Suite		Anmerkung
		myAgent	myReports	
Agenten, Warteschlangen und Zeitpläne	-	x	-	
Fax und E-Mail	-	x	-	
vordefinierte Reports/ Berichtsvorlagen	-	x	x	
Berichts-Designer für eigene Reports/Berichts-vorlagen	-	-	x	
zeitgesteuertes Erstellen von Reports/Berichten	-	-	x	

Optional ist die Anschaltung von OpenScape Contact Center möglich.

Attendants (Vermittlungsplätze)

UC-Funktion	UC Smart	UC Suite	Anmerkung
	Business Attendant	myAttendant	
Anzeige wartender Anrufe mit Anrufart,? Name und Rufnummer	x	x	
Anzeige des Verbindungsstatus	x	x	
Schnelle Vermittlung von Anrufen	x	x	
Kurzwahl über Belegtfelder/Benutzerschaltflächen. Individuelle Konfiguration der Belegtfelder/Benutzerschaltflächen mit Rufnummer oder Name	x	x	
Anwesenheitsstatus von anderen Teilnehmern sehen	x	x	Bei OpenStage Business Attendant wird für Präsenz UC Booster Card/Server oder Business S benötigt
Anwesenheitsstatus von anderen Teilnehmern ändern	x	x	
Persönliches Verzeichnis	-	x	
Internes Verzeichnis	x	x	
Externes Verzeichnis	x	x	
Outlook-Kontakte	x	x	
LDAP-Zugriff	x	x	
Journal	-	x	
AdHoc-Konferenz	x	x	

UC-Funktion	UC Smart	UC Suite	Anmerkung
	Business Attendant	**myAttendant**	
geplante, permanente und offene Konferenzen (Drag&Drop-Konferenz)	-	x	
Nachrichtencenter	-	x	Im Nachrichten-Center werden Sprach-, Fax- und Sofortnachrichten, sowie SMS und E-Mails protokolliert und verwaltet
Zugriff auf Sprach- und Faxnachrichten von anderen Teilnehmern	-	x	Muss vom jeweiligen Teilnehmer freigeschaltet werden
Instant Messaging (Chat)	-	x	
Nachtschaltung	x	x	
BLF/BLF-Server	x	x	In einer Vernetzung ist Präsenz nur über BLF-Server möglich

Der empfohlene Attendant Client für UC Suite ist myAttendant. OpenScape Business Attendant kann aber auch mit UC Suite verwendet werden.

Voicemail & Company AutoAttendant

UC-Funktion	UC Smart	UC Suite	Anmerkung
UC Smart Voicemail & Company AutoAttendant Basisfunktionalität	x	-	
UC Suite Voicemail & Company AutoAttendant Basisfunktionalität	-	x	UC Booster Card/Server oder Business S benötigt
UC-Funktionen			
Grafische Bedienung der Voicemail für Teilnehmer (Web-Interface bzw. Client-Oberfläche)	x	x	
Voicemail-Ansagen für Präsenzfunktion	x	x	Unterschiedliche Ansagen je eingestellter UC Präsenz
Persönliche Regeln für Begrüßungen pro Mailbox	-	x	Teilnehmer legt detaillierte Regeln für die Auswahl seiner persönlichen Ansagen fest
Voicemail to E-Mail	x	x	Voicemail wird als Wave-Datei an E-Mail angehängt
AutoAttendant-Funktionen			
Vermittlungs-Mailboxen (Basic AutoAttendants)	100	20	
Company Auto Attendant	x	x	Zentraler Vermittlungsplatz und zentrale Voicemail mit alternativen Ansagen je Nebenstelle

UC-Funktion	UC Smart	UC Suite	Anmerkung
Ansagen vor Melden / Parallel-Signalisierung	x	x	Ansage zum Anrufer während der Teilnehmer angerufen wird bei UC Suite ist das nur in Verbindung mit dem Contact Center möglich
Einwahlziele für 4 Tagesabschnitte / Kalender für AutoAttendant	x	x	Automatische Vermittlung unterschiedlich zu verschiedenen Tageszeiten Kalender-Funktion bei UC Smart über die automatische Nachtschaltung möglich
Kalender zentral für Mailbox	x	x	Ansagen und Rufbehandlung für firmenweite Termine z.B. Feiertage, Betriebsferien etc.
Profile individuell für Mailbox und pers. Auto-Attendant	-	x	Präsenzabhängige Rufbehandlung individuell je Teilnehmer einstellbar
Zeitpläne	Tag-Nachschaltung	Zeitplan mit Regeln (Call Control Vector CCV)	
Templates	1 AutoAttendant standardmäßig eingerichtet	5 anpassbare Vorlagen	
grafischer Regel-Editor (CCV-Editor)	-	x	
Verkettung von Mailboxen / Multi Step Auto-Attendant	x	-	Das Gespräch wird von einer verketteten Mailbox auf die nächste weitergeleitet und dabei wird immer die jeweilige Ansage abgespielt
Nach Name wählen (Dial by Name)	-	x	
Nebenstellenwahl (Dial by Extension)	x	x	
Voicemail-Funktionen			
Individuelle Begrüßungen pro Mailbox	4	10	Verschiedene Ansagen speichern und einstellen
Weiterleitung von Sprachnachrichten	-	x	Nachricht an andere Teilnehmer/Mailboxen weiterleiten
Rückruf aus der Voicebox	x	x	Rückruf zum Anrufer der Nachricht aktivierbar
Benachrichtigungsruf	-	x	Wenn eine Nachricht vorliegt erfolgt ein Ruf zu einem externen Ziel, z. B. Handy
Vertreterfunktion	-	x	Weiterleitung des Anrufers an Vertreter mit persönlicher Ansage

UC-Funktion	UC Smart	UC Suite	Anmerkung
Anruferbasierte Voicemail / CLI-Routing	-	x	Behandlung von Rufnummer abhängig, z. B. Begrüßung in Anrufersprache
Zentrale Gruppen-Mailbox	x	x	mit Ansagen für Abteilungen/ Gruppen
Mitschneiden / Live Recording	-	x	Mitschneiden von Gesprächen mit Sicherheitsfunktionen
Nachrichten speichern	-	x	Teilnehmer können einzelne Voicemail-Nachrichten für sich abspeichern
Automatisches Löschen von Nachrichten	x	x	Nach Zeit werden Nachrichten gelöscht, um Speicher frei zu machen
Mailbox-Sprachwechsel teilnehmerindividuell	-	x	Auswahl der autom. Ansagen in individueller Sprache

2.2.2 Benutzerzugriff auf UC-Funktionen (UC Clients)

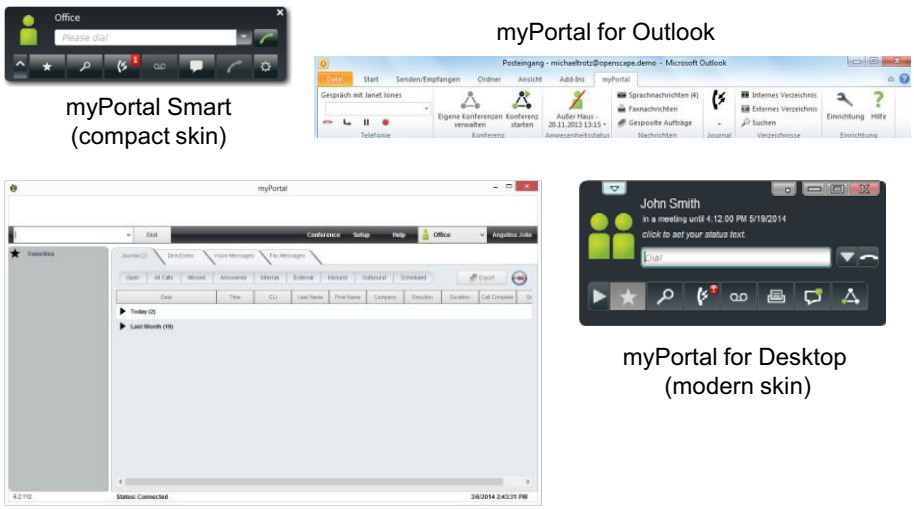
Der Zugriff der UC-Funktionen erfolgt über UC Clients. Auf Anwesenheitsstatus (UC Suite) und Sprachbox (UC Smart und UC Suite) kann auch über TUI (Telefonie User Interface) zugegriffen werden.

UC Clients werden für die gängigen Betriebssysteme angeboten. Bitte beachten Sie hierzu auch die Voraussetzungen der Clients in den jeweiligen Freigabemitteilungen.

Communication Clients (Desktop und Groupware Clients)

Client	empfohlen für		Beschreibung
	UC Smart	UC Suite	
myPortal Smart	x	-	UC-Desktop-Client für Microsoft Windows und Apple Mac
myPortal for Desktop	-	x	Erweiterter UC-Desktop-Client für Microsoft Windows und Apple Mac
myPortal for Outlook	-	x	UC-Groupware-Client für Microsoft Outlook-Integration
myPortal for OpenStage	x	x	Präsenz- und VoiceMail-Steuerung bei UC Suite Präsenz-Steuerung bei UC Smart für OpenStage 60 HFA und OpenScape Desk Phone IP 55G HFA Telefone

Bild: myPortal Smart, myPortal for Desktop und myPortal for Outlook



Mobility Clients

Client	empfohlen für		Beschreibung
	UC Smart	UC Suite	
myPortal for Mobile myPortal for Tablet	x	x	Mobility-Clients für Mobiltelefon und Tablet-PC myPortal for Mobile ist mit leicht unterschiedlichem Funktionsumfang für UC Smart und UC Suite verfügbar
myPortal to go	x	x	Mobile App für Smartphones myPortal to go ist mit leicht unterschiedlichem Funktionsumfang für UC Smart und UC Suite verfügbar

Bild: myPortal for Mobile/Tablet



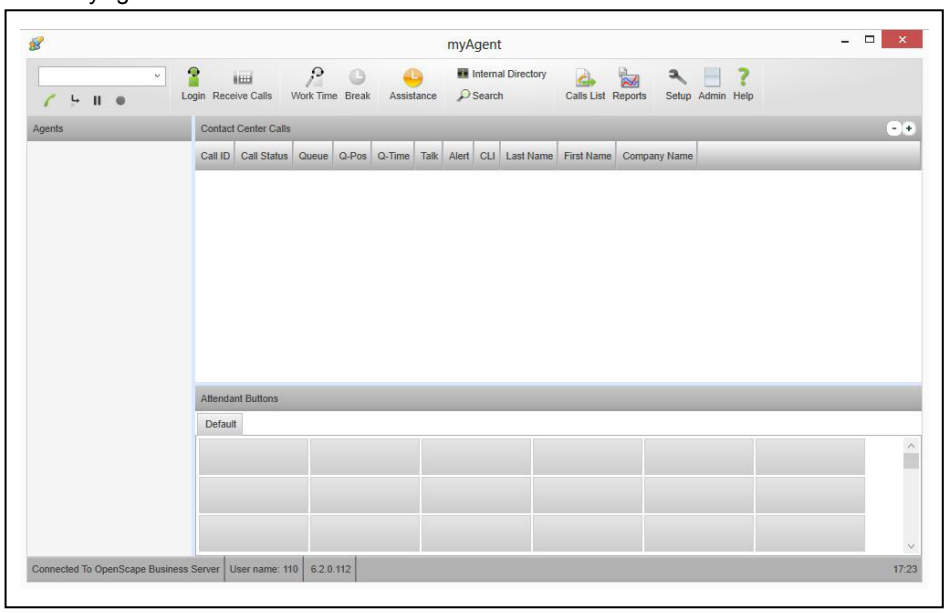
Bild: myPortal to go



Contact Center Clients

Client	empfohlen für		Beschreibung
	UC Smart	UC Suite	
myAgent	-	x	Contact Center Client
myReports	-	x	Reports/Auswertungsoberfläche für Contact Center myReports kann unabhängig vom Contact Center auch für System-statistiken eingesetzt werden

Bild: myAgent



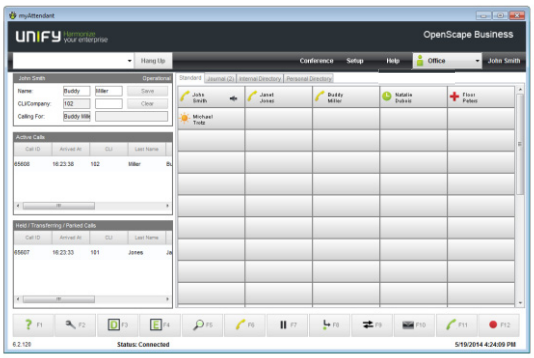
Attendants/Vermittlungsplätze

Client	empfohlen für		Beschreibung
	UC Smart	UC Suite	
OpenScape Business Attendant	x	-	UC-Vermittlungsplatz inklusive Präsenz
myAttendant	-	x	Erweiterter UC-Vermittlungsplatz für UC Suite

Bild: myAttendant



Business Attendant



myAttendant

2.2.3 Integration in Geschäftsanwendungen

OpenScape Business kann in bestehende IT-Infrastrukturen und Geschäftsanwendungen integriert werden.

Applikationen

- Application Launcher für eine aktive Interaktion mit CRM/ERP-Applikationen
- Accounting Software für Gebührenauswertungen

Integrierte Services

- Directory Services für Informationen zu Anrufern und der Suche in internen und externen Verzeichnissen
- Präsenz-Management und IM (Instant Messaging) über XMPP zu sozialen Netzwerken (Social Media Networks)
- Web Services für Interaktionen mit Web-basierten Applikationen auf z. B. Mobiletelefonen und Tablet-PC

CTI-Middleware

- First- and Third-party TAPI Service Provider für die Anrufsteuerung aus CTI- oder CRM/ERP-Applikationen

Schnittstellen und Protokolle

- CSTA für die Überwachung und Steuerung unterschiedlichster Applikationen
- SIP für die Verbindung zu SIP-Trunking basierten Applikationen
- LDAP für die Verbindung zu externen Verzeichnissen oder von externen LDAP-Clients
- HTTP und HTTPS für den Zugriff auf UC-Funktionen des integrierten Web-Servers

- TCP/IP als Basisprotokoll für alle Ethernet-Verbindungen
- SQL Konnektor für die Anschaltung von SQL-Datenbanken (Microsoft SQL Server, PostgreSQL, Sybase SQL Server)
- LDAP Konnektor für externe LDAP-Server wie z. B. Active Directory

2.3 OpenScape Business Modelle

Für die Nutzung der Telefonie und UC-Funktionen werden unterschiedliche Modelle angeboten. Sie können zwischen Hardwaremodellen und reinen Softwaremodellen wählen, die auf Standard Servern oder in einer virtuellen Umgebung mit VMware vSphere betrieben werden.

Die UC-Funktionalität für UC Smart ist bereits auf dem Mainboard der OpenScape Business X integriert. UC Suite benötigt zusätzlich entweder die Baugruppe UC Booster Card oder den externen UC Booster Server. Oder Sie wählen den Softswitch OpenScape Business S mit integrierter UC Suite.

2.3.1 Vertriebliche Ausbaustufen

Die OpenScape Business Modelle haben unterschiedliche Ausbaustufen.

	X1	X3		X5		X8	Server (S)
	Wand	Rack	Wand	Rack	Wand		
Anbindung an Service-Provider							
ITSP-Kanäle (SIP-Provider)	30	60	60	60	60	60	128
max. Anzahl SIP-Provider	4	4	4	4	4	4	4
ISDN S_0 (BRI)	4	20	20	52	52	128	-
	via Mainboard	2* STSLX4		6* STLSX4		SW-Limit, d. h. unabhängig von der Anzahl der STDM3-Baugruppen	
ISDN S_{2M} (PRI)	-	-	-	30	30	180	-
				1* TS2		3* DIUT2	
Max. Anzahl Leitungskanäle	250	250	250	250	250	250	250
Teilnehmer							
Analoge	4	20	20	52	68	384	-
	via Mainboard	2* SLAD8	1* SLAD16	6* SLAD8	4* SLAD16	16* SLMA	
Digitale	8	24	24	56	56	384	-
	via Mainboard	2* SLU8		6* SLU8		16* SLMO2	
IP-Teilnehmer	20[1]	500	500	500	500	500	500

	X1	X3		X5		X8	Server (S)
	Wand	**Rack**	**Wand**	**Rack**	**Wand**		
Cordless/DECT(CMI)	16	32	32	32	32/64	250	-
	1-7 Basisstationen via Mainboard	1-7 Basisstationen via Mainboard	1-7 Basisstationen via Mainboard	1-7 Basisstationen via Mainboard	64 mit 1* SLC16N nur in der X5W	4* SLCN	
Max. Anzahl Teilnehmer	30	500	500	500	500	500	500
Unified Communications (UC Smart)							
myPortal Smart	30	50	50	50	50	50	-
Smart VoiceMail (Smart VM)	30	320	320	320	320	320	-
Anzahl Mobility Entry User	30	150	150	150	150	150	-
myPortal for Mobile/Tablet	30 einrichtbar / 30 parallel aktiv	50 einrichtbar / 30 parallel aktiv	50 einrichtbar / 30 parallel aktiv	50 einrichtbar / 30 parallel aktiv	50 einrichtbar / 30 parallel aktiv	50 einrichtbar / 30 parallel aktiv	-
myPortal to go	30	50	50	50	50	50	-
Max. Anzahl der mobilen Teilnehmer	30	150	150	150	150	150	-
OpenScape Business Attendant	8	8	8	8	8	8	8
OpenScape Business BLF	30	50	50	50	50	50	50
	Max. 350 BLF Tasten	Max. 350 BLF Tasten	Max. 350 BLF Tasten	Max. 350 BLF Tasten	Max. 350 BLF Tasten	Max. 350 BLF Tasten	Max. 350 BLF Tasten
Unified Communications (UC Suite)							
Max. Anzahl gleichzeitig aktiver UC Suite CIlents	-	500/150[2]	500/150[2]	500/150[2]	500/150[2]	500/150[2]	500
myPortal for Desktop	-	500/150[2]	500/150[2]	500/150[2]	500/150[2]	500/150[2]	500
myPortal for Outlook	-	500/150[2]	500/150[2]	500/150[2]	500/150[2]	500/150[2]	500
VoiceMail	-	500	500	500	500	500	500
Anzahl Mobility Entry User	-	150	150	150	150	150	-
myPortal for Mobile/Tablet	-	100 einrichtbar / 30 parallel aktiv	100 einrichtbar / 30 parallel aktiv	100 einrichtbar / 30 parallel aktiv	100 einrichtbar / 30 parallel aktiv	100 einrichtbar / 30 parallel aktiv	200 einrichtbar / 30 parallel aktiv
myPortal to go	-	100	100	100	100	100	200 einrichtbar / 100 parallel aktiv
Max. Anzahl der mobilen Teilnehmer	-	150	150	150	150	150	200
myAgent	-	192 einrichtbar / 64 parallel aktiv	192 einrichtbar / 64 parallel aktiv	192 einrichtbar / 64 parallel aktiv	192 einrichtbar / 64 parallel aktiv	192 einrichtbar / 64 parallel aktiv	192 einrichtbar / 64 parallel aktiv
myReports	-	1	1	1	1	1	1

	X1	X3		X5		X8	Server (S)
	Wand	Rack	Wand	Rack	Wand		
myAttendant	-	20	20	20	20	20	20
Max. Anzahl Fax Kanäle	-	3	3	3	3	3	3
Max. Anzahl Fax User	-	200/150[2]	200/150[2]	200/150[2]	200/150[2]	200/150[2]	200
Max. Anzahl Kanäle für Konferenzen	-	20	20	20	20	20	40
Unified Communications (CRM, Datenbankanbindung)							
Application Launcher	30 einrichtbar / 30 parallel aktiv	500 einrichtbar / 50 parallel aktiv	500 einrichtbar / 50 parallel aktiv	500 einrichtbar / 50 parallel aktiv	500 einrichtbar / 50 parallel aktiv	500 einrichtbar / 50 parallel aktiv	500 einrichtbar / 50 parallel aktiv
TAPI 120/170 User (über CSTA, UC Booster Server/ Card notwendig)	-	500/150[2]	500/150[2]	500/150[2]	500/150[2]	500/150[2]	500
TAPI 120 User (im UC Smart Modus via Mainboard ohne CSTA)	30	30	30	30	30	30	
Directory Service Connector (UC Booster Card/Server notwendig)	-	4	4	4	4	4	4
Gate View							
Kameras	-	8/2[2]	8/2[2]	8/2[2]	8/2[2]	8/2[2]	8

1 max. Summe aus IP und Deskshare User = 20 (Begrenzung über Konfiguration) - max. Summe aus IP, Deskshare, analogen und digitalen Teilnehmern = 30 (Begrenzung über Lizenzen)

2 1. Wert: Maximaler Ausbau mit UC Booster Server (ab 150 UC Suite Benutzer) / 2. Wert: Maximaler Ausbau mit UC Booster Card (bis 150 UC Suite Benutzer)

Für eine detaillierte Beschreibung der Ausbaustufen/Ausbaugzenzen siehe auch *Ausbaugrenzen und Kapazitäten*).

OpenScape Business UC-Vernetzung

OpenScape Business bietet weitreichende UC-Vernetzungsmöglichkeiten:

- Umfassende Voice- und UC-Vernetzung zwischen den verschiedenen OpenScape Business X (bei UC-Vernetzung UC Booster Card/Server notwendig) und OpenScape Business S
- mit mehreren Gebäuden auf dem Firmengelände
- mit verteilten Standorten
- zentrale Administration inkl. Lizenzen (HiPath 5000 RSM nicht mehr notwendig)
- Voice-Vernetzung mit OpenScape Enterprise in Vorbereitung

Bei Voice-Vernetzung werden Vernetzungen mit bis zu 32 Knoten unterstützt. Bei UC-Vernetzung werden Vernetzungen mit maximal 8 Knoten und bis zu 1000 Teilnehmern unterstützt. Darüber hinaus sind projektspezifische Freigaben möglich.

Für eine detaillierte Beschreibung der Vernetzungsszenarien siehe *Ausbaugrenzen und Kapazitäten*).

2.3.2 UC Hardware Modelle

Die Kommunikationssysteme OpenScape Business X bieten ein hohes Maß an Flexibilität hinsichtlich Leistungsumfang und Konstruktion. Je nach OpenScape Business X Modell werden bis zu 500 Teilnehmer für IP, Digital (ISDN), Analog (a/b) und Cordless (DECT) sowie die Anbindung ans öffentliche Netz über ITSP (SIP), ISDN (BRI und PRI), CAS und Analog und onboard-IP (auf dem Mainboard vorgeleistet) unterstützt.

- OpenScape Business X1
  Kommunikationssystem im Wandgehäuse, das an einer Wand montiert werden muss.
- OpenScape Business X3W
  Kommunikationssystem im Wandgehäuse, das an einer Wand montiert werden muss.
- OpenScape Business X3R
  Kommunikationssystem im 19"-Rackgehäuse, das in einen 19"-Schrank montiert, frei aufgestellt (Tischbetrieb) oder an einer Wand montiert werden kann.
- OpenScape Business X5 W
  Kommunikationssystem im Wandgehäuse, das an einer Wand montiert werden muss.
- OpenScape Business X5R
  Kommunikationssystem im 19”-Rackgehäuse, das in einen 19”-Schrank montiert, frei aufgestellt (Tischbetrieb) oder an einer Wand montiert werden kann.
- OpenScape Business X8
  Modulares Kommunikationssystem, das als Einboxsystem (Basisbox) oder als Zweiboxsystem (Basisbox + Erweiterungsbox) eingesetzt werden kann. Das Kommunikationssystem kann frei aufgestellt oder in einen 19"-Schrank montiert werden.

Bild: Hardware-Plattformen



2.3.3 UC Booster Hardware

UC Booster Hardware für OpenScape Business X.

- OpenScape Business UC Booster Card
  Baugruppe für OpenScape Business X, wenn UC Suite als UC-Lösung mit bis zu 150 UC-Benutzern eingesetzt werden soll.
- OpenScape Business UC Booster Server
  Externer UC Booster Server (Linux-Server) für OpenScape Business X, wenn UC Suite als UC-Lösung mit bis zu 500 UC-Benutzern eingesetzt werden soll. Auf dem UC Booster Server wird SLES 11 SP3 64 Bit verwendet. Der UC Booster Server kann auch in einer virtuellen Umgebung mit VMware vSphere betrieben werden.
  Bei Einsatz des UC Booster Servers wird die UC Booster Card nicht benötigt.
- OpenScape Business Voice Channel Booster Card
  Zwei Options-Baugruppen zur Erweiterung von OpenScape Business X mit zusätzlichen DSP-Kanälen (z. B. für gleichzeitige Sprachverbindungen mit IP/TDM-Übergängen).
  Auf dem Mainboard sind 8 DSP-Kanäle vorgeleistet. Die Voice Channel Booster Card OCCB/1 bietet weitere 48 DSP-Kanäle und die Voice Channel Booster Card OCCB/3 bis zu 128 DSP-Kanäle.

2.3.4 UC Software Modelle (Softswitch)

All-In-One Server-basierte UC-Software-Lösung mit Unterstützung für bis zu 500 IP-Teilnehmer und Anbindung ans öffentliche Netz über ITSP (SIP).

OpenScape Business S kann plattformunabhängig auf einem Linux-Server installiert werden. Als Betriebssystem wird SLES 11 SP3 64 Bit verwendet. OpenScape Business S kann auch in einer virtuellen Umgebung mit VMware vSphere betrieben werden. Wenn TDM-Schnittstellen zur Anbindung von TDM-Endgeräten oder TDM-Leitungen benötigt werden, können OpenScape Business X Systeme als Gateway eingesetzt werden.

2.3.5 Aufbau und Umweltbedingungen

	X1	X3W	X3R	X5W	X5R	X8
Aufbau	Wandsystem	Wandsystem	Rack	Wandsystem	Rack	Standardsystem (auch Einbau in Rack möglich)
Abmessungen (HxBxT in mm)	470x370x80	450x460x130	89x440x380 (2U)	450x460x200	155x440x380 (3,5U)	490x440x430
Gewicht	ca. 2,8 kg	ca. 6 kg	ca. 6 kg	ca. 8 kg	ca. 8 kg	ca. 34 kg (voll bestückt)
Gehäusefarbe	Weiß	Weiß	Grün/Dunkelgrau	Weiß	Grün/Dunkelgrau	Grün/Dunkelgrau
Stromversorgung	Die Modelle sind standardmäßig für den Netzbetrieb ausgelegt • Nenneingangsspannung (AC): 100 bis 240 V • Nennfrequenz: 50/60 Hz • Batteriespeisung (DC): -48 V					
Leistungsaufnahme	Abhängig von der Hardware-Plattform und dem Ausbau					
Umweltbedingungen	• Betriebsbedingungen: +5 bis +40 °C (41 bis 104 °F) • Luftfeuchtigkeit: 5 bis 85%					

2.3.6 Unterstützte Telefone

OpenScape Business X ermöglicht Telefonieren über IP/HFA (HiPath Feature Access), SIP, TDM, a/b, Cordless/DECT und WLAN. An OpenScape Business S können IP-/HFA-, SIP- und WLAN-Telefone angeschlossen werden.

OpenStage-Telefone (IP/ HFA, SIP und T))	• OpenStage 5/10/15/20/30/40/60/80
OpenScape Desk Phone (IP/ HFA, SIP)	• OpenScape Desk Phone IP 35G/55G • OpenScape Desk Phone IP 35G Eco SIP
Beistellgeräte	• OpenStageKey Module nur für OpenStage 15/40/60 • OpenStage BLF 40 (Busy Lamp Field) nur für OpenStage 40 und OpenStage 30 T
Cordless/CMI/DECT-IP/ DECT-Telefone	• OpenStage S4/SL4/M3
PC-Clients (HFA, SIP)	• OpenScape Personal Edition (bei SIP inkl. Video)
SIP-Telefone (UC Suite) / AP-Adapter	• SIP-Telefone mit RFC 3725-Unterstützung • Mediatrix 4102S (zum Anschluss von 2 analogen Telefonen oder Faxgeräten)
WLAN-Telefone	• OpenStage WL3
Analog- und ISDN-Telefone	• analoge (a/b) Telefone • digitale (S_0) ISDN-Telefone

Ältere Geräte (z. B. optiPoint 410/420/500, Gigaset SL3/S3/M2, optiPoint WL2 SIP) werden unterstützt. Optiset E-Geräte können nicht betrieben werden.

Funktionen und Konfiguration der SIP-Telefone

OpenScape Business bietet für OpenStage HFA Telefone einen umfangreichen Funktionsumfang für die Sprachkommunikation. Viele Funktionen sind auch für Standard-SIP-Telefone möglich.

Eine Übersicht der mit OpenStage SIP-Telefonen unterstützen Leistungsmerkmale und weitere Hinweise finden Sie im Unify Wiki unter dem Link

`http://wiki.unify.com/wiki/Features_and_Configuration_of_SIP_Devices`

Für die Steuerung von Sprachverbindungen für SIP Telefone über CTI (3PCC) wird bei OpenScape Business X3/X5/X8 eine UC Booster Card oder ein UC Booster Server benötigt.

Die Steuerung von Sprachverbindungen für SIP Telefone über UC Smart Clients wird für OpenScape Business X3/X5 Rack mit UC Booster Card unterstützt.

Mit Hilfe der DLI-Funktionen können die OpenScape Desk Phone (SIP) Telefone zentral administriert und mit Software versorgt werden.

2.4 Weiterführende Informationen

Weiterführende Informationen finden Sie im Internet und Extranet. Für Einschränkungen und letzte Änderungen beachten Sie auch die Freigabemitteilungen.

2.4.1 Unterstützte Sprachen

Für die unterschiedlichen Softwarekomponenten (Clients und WBM) und Dokumentation/Online-Hilfe stehen verschiedene Sprachen zur Verfügung.

Die folgenden Sprachen werden im Rahmen der Ländereinführungen bereitgestellt.

	de en	**es fr it nl pt**	**da no sv**	**fi**	**ru**	**cs**	**pl**	**hr tr**	**hu**	**zh**
UC Smart Clients										
myPortal Smart (Client)	X	X	X	X	X	X	X	X	X	–
myPortal Smart (Bedienungsanleitung)	X	X	–	–	–	–	–	–	–	–
myPortal for Mobile (Client)	X	X	X	X	X	X	X	X	X	–
myPortal for Mobile (Bedienungsanleitung/Online-Hilfe)	X	X	X	X	X	X	X	–	–	–
myPortal to go (Client)	X	X	X	X	X	X	X	X	X	–
myPortal to go (Bedienungsanleitung/Online-Hilfe)	X	X	X	X	X	X	X	–	–	–
myPortal for OpenStage (Telefon)	X	X	X	X	X	X	X	X	X	–
myPortal for OpenStage (Bedienungsanleitung)	X	X	–	–	–	–	–	–	–	–
TUI (Telephone User Interface)	X	X	X	X	X	X	–	X	–	X
TUI (Kurzbedienungsanleitung)	X	X	–	–	–	–	–	–	–	–
OpenScape Business Attendant / BLF (Client)	X	X	–	–	–	X	–	–	–	–
OpenScape Business Attendant / BLF (Bedienungsanleitung)	X	X	–	–	–	X	–	–	–	–
UC Suite Clients										
myPortal for Desktop (Client)	X	X	X	X	X	X	X	X	X	X
myPortal for Desktop (Bedienungsanleitung/Online-Hilfe)	X	X	X	X	X	X	X	–	–	–
myPortal for Outlook (Client)	X	X	X	X	X	X	X	X	X	X
myPortal for Outlook (Bedienungsanleitung/Online-Hilfe)	X	X	X	X	X	X	X	–	–	–
myPortal for Mobile (Client)	X	X	X	X	X	X	X	X	X	–
myPortal for Mobile (Bedienungsanleitung/Online-Hilfe)	X	X	X	X	X	X	X	–	–	–
myPortal to go (Client)	X	X	X	X	X	X	X	X	X	–
myPortal to go (Bedienungsanleitung/Online-Hilfe)	X	X	X	X	X	X	X	–	–	–
myPortal for OpenStage (Client)	X	X	X	X	X	X	X	X	X	–

	de en	es fr it nl pt	da no sv	fi	ru	cs	pl	hr tr	hu	zh
myPortal for OpenStage (Bedienungsanleitung)	X	X	–	–	–	–	–	–	–	–
myAttendant (Client)	X	X	X	X	X	X	X	X	X	X
myAttendant (Bedienungsanleitung/Online-Hilfe)	X	X	X	X	X	X	X	–	–	–
myAgent (Client)	X	X	X	X	X	X	X	X	X	X
myAgent (Bedienungsanleitung/Online-Hilfe)	X	X	X	X	X	X	X	–	–	–
myReports (Client)	X	X	–	X	X	X	X	–	–	–
myReports (Bedienungsanleitung/Online-Hilfe)	X	X	–	X	X	X	X	–	–	–
TUI (Telephone User Interface)	X	X	X	X	X	X	X	X	X	X
TUI (Kurzbedienungsanleitung)	X	X	–	–	–	–	–	–	–	–
Administration										
OpenScape Business Assistant (WBM)	X	X	–	–	–	–	–	–	–	–
OpenScape Business Assistant (Administratordokumentation/Online-Hilfe)	X	X (kein nl)	–	–	–	–	–	–	–	–
Manager E	X	X	X	X	X	X	X	–	–	–
Manager E (Administratordokumentation/Online/Hilfe)	X	X	–	–	X	–	–	–	–	–

Zusätzlich wird die UC Smart TUI auch in den Sprachen Belgisch (flämisch) und Slowenisch angeboten.

INFO: Ein russisches bzw. chinesisches Windows-Betriebssystem ist Voraussetzung, um die russische bzw. chinesische Bedienoberfläche nutzen zu können.

Bei den in der Tabelle verwendeten Abkürzungen handelt es sich um folgende Sprachcodes (ISO 639-1):

- de = Deutsch
- en = Englisch
- cs = Tschechisch
- da = Dänisch
- es = Spanisch
- fi = Finnisch
- fr = Französisch
- hr = Kroatisch
- hu = Ungarisch
- it = Italienisch
- nl = Niederländisch

- no = Norwegisch
- pl = Polnisch
- pt = Portugiesisch
- ru = Russisch
- sv = Schwedisch
- tr = Türkisch
- zh = Chinesisch

2.4.2 Internet-Links

Weitere Informationen und ggf. aktuellere Informationen finden Sie auf der Unify Homepage, in unserem Experten-Wiki und im Unify Partnerportal.

Internet-Links

- Unify Homepage:
  `http://www.unify.com`
- Experten-Wiki für Telefone, Kommunikationssysteme und UC:
  `http://wiki.unify.com`
- Partnerportal (Registrierung erforderlich):
  `https://www.unify.com/de/partners/partner-portal.aspx`
  oder
  `https://www.unify.com/en/partners/partner-portal.aspx`

3 Administrationskonzept

Die Administration des Kommunikationssystems erfolgt mit dem OpenScape Business Assistant. Einige spezielle Administrationsaufgaben erfordern den Manager E.

3.1 OpenScape Business Assistant (WBM)

Der OpenScape Business Assistant ist webbasiert und wird daher auch Web Based Management (WBM) genannt.

Der Umfang der angebotenen Administrationsaufgaben ist abhängig vom verwendeten Addministratorprofil.

Zu jeder Seite des WBM steht eine Online-Hilfe zur Verfügung.

3.1.1 Voraussetzungen für das WBM

Um das WBM nutzen zu können, benötigt der Administrations-PC geeignete Software.

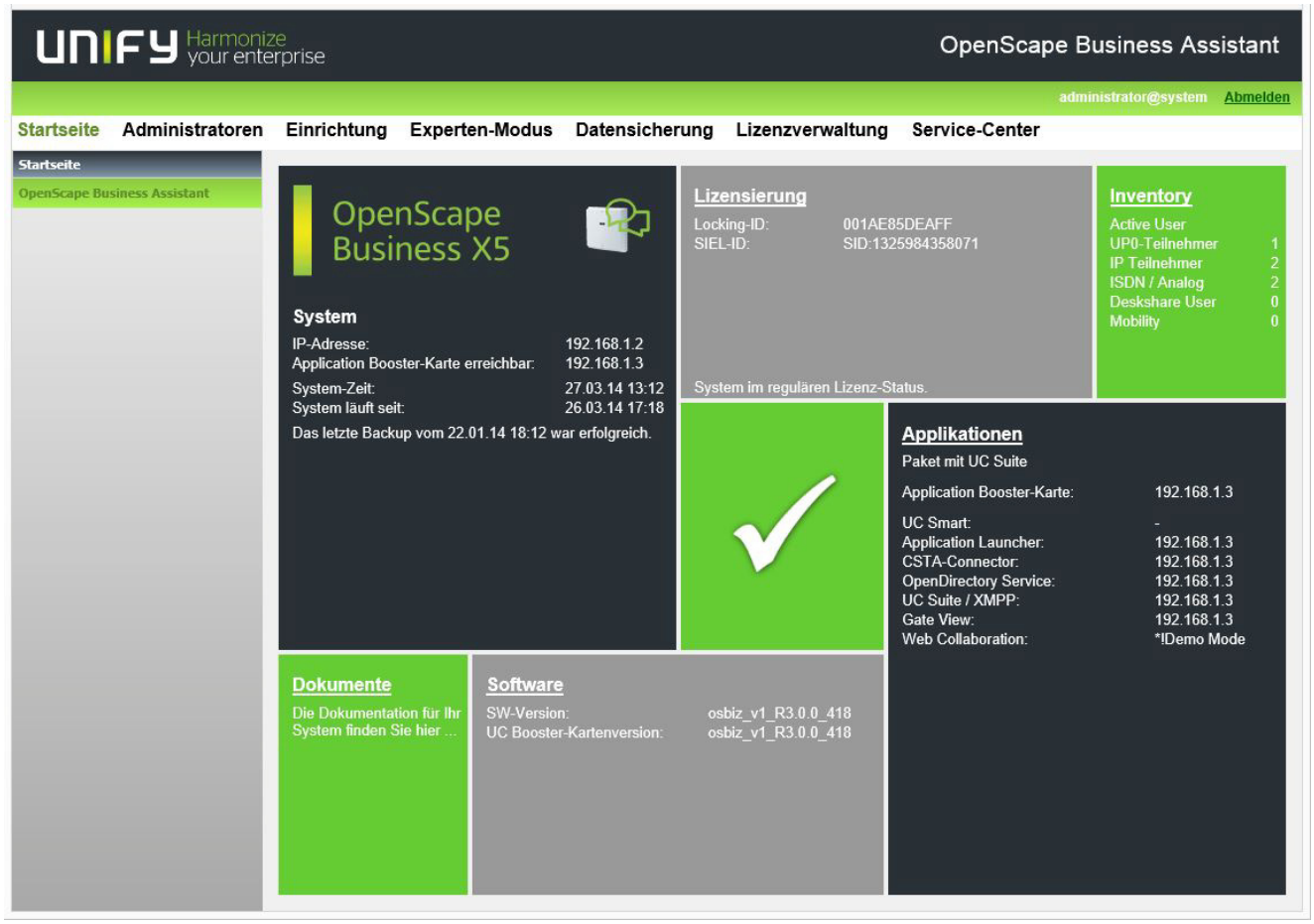
Unterstützte Webbrowser:

- Microsoft Internet Explorer 10 oder neuer
- Mozilla Firefox 18 oder neuer

3.1.2 Startseite des WBM

Die Startseite des WBM zeigt wichtige Systeminformationen an, die in verschiedene Bereiche (Kacheln) aufgeteilt sind. Zusätzlich gibt sie Hinweise und informiert über Systemfehler, Ereignisse und Aktionen.

Die angebotenen Systeminformationen sind abhängig vom verwendeten Administratorprofil. Die unterstrichenen Überschriften in den einzelnen Bereichen sind anklickbar und verweisen auf das zugehörige Thema im WBM.



Folgende Informationen werden angezeigt:

- Bereich **Status** (Mitte)
  - weißes Häkchen auf grünem Hintergrund: das Kommunikationssystem ist voll funktionsfähig - rot hinterlegte Meldungen in den anderen Feldern weisen auf Aktionen hin, die durchgeführt werden sollten.
  - weißes Häkchen auf rotem Hintergrund: das Kommunikationssystem ist nicht voll funktionsfähig und erfordert den Eingriff des Administrators - rot hinterlegte Meldungen in den anderen Feldern weisen auf Systemfehler oder Ereignisse hin, die behoben werden müssen.
- Bereich **System**
  - Produkt
  - IP-Adresse des Kommunikationssystems
  - Aktuelles Datum und Uhrzeit
  - Datum und Uhrzeit der letzten Softwareaktualisierung
  - Hinweise beim Betrieb in einem Netzverbund (System ist Master oder Slave, Anzeige der Knoten-ID)
  - Synchronisierungs-Status
  - Hinweise für Sichern und Wiederherstellen
- Bereich **Dokumente**

  - Verlinkung auf die Dokumentation
- Bereich **Software**
  - Version der installierten Software des Kommunikationssystems
  - Anzeige, ob eine UC Booster Card gesteckt ist. Ist sie zusätzlich über eine IP-Adresse erreichbar, wird die Version der installierten UC Booster Card Software angezeigt.
    UC Booster Card und Kommunikationssystem sollten immer auf dem gleichen Softwarestand sein.
  - Hinweis auf neue Softwareversion
- Bereich **Lizenzierung**
  - Locking ID für die Lizenzierung
  - SIEL-ID für die Lizenzierung
  - Hinweis auf den Lizenzierungszustand
- Bereich **Inventory**
  - Typ und Anzahl der aktiven Teilnehmer
- Bereich **Applikationen**
  - Verwendetes Applikationspaket (UC Smart oder UC Suite) und dessen Komponenten inkl. der IP-Adressen der verwendeten Server.
  - Anzeige, ob eine UC Booster Card gesteckt ist.

3.1.3 Einführung in das WBM

Das WBM ist die webbasierte Anwendung für die Administration des Systems.

Sprache der Benutzeroberfläche

Sie können beim Anmelden eine der folgenden Sprachen wählen:

- Deutsch
- Englisch
- Französisch
- Italienisch
- Niederländisch (Online-Hilfe nur Englisch verfügbar)
- Portugiesisch
- Spanisch

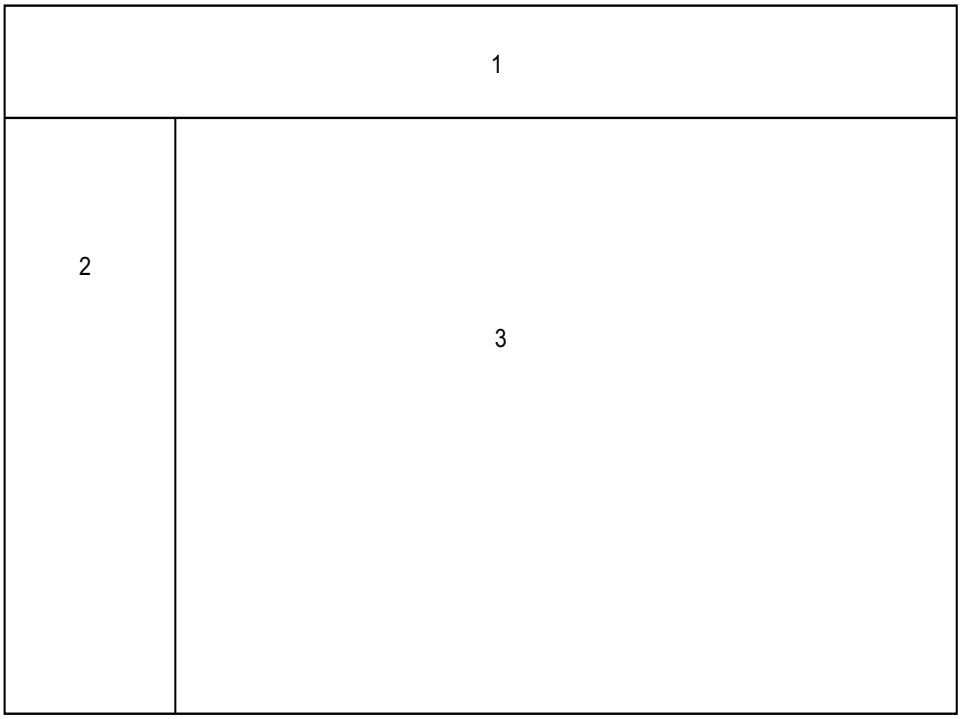
Rangfolge der beschriebenen Benutzeroberflächen

Sämtliche Tasks, die in einem Wizard durchgeführt werden können, sind nur für den entsprechenden Wizard beschrieben.

Weitere Tasks, die im Experten-Modus durchgeführt werden können, sind nur für den Experten-Modus beschrieben.

Nur die übrigen Tasks sind für Manager E beschrieben.

Elemente der Benutzeroberfläche



- Navigationsleiste (1)
  Die Navigationsleiste ist die Primärnavigation und zeigt stets dieselben Links zu den Aufgaben-Centern **Startseite**, **Administratoren**, **Einrichtung**, **Experten-Modus**, **Datensicherung**, **Lizenzverwaltung** und **Service-Center** sowie den aktuellen Benutzernamen und den Link **Abmelden**. Nach Anklicken eines Aufgaben-Centers öffnet sich im Navigationsbereich der zugehörige Navigationsbaum und im Arbeitsbereich die Startseite des Aufgaben-Centers.
- Navigationsbereich (2)
  Der Navigationsbereich ist die Sekundärnavigation und enthält den Navigationsbaum mit den Menüpunkten des gewählten Aufgaben-Centers. Im Navigationsbaum wird an oberster Stelle der Name des gewählten Aufgaben-Centers angezeigt. Darunter befinden sich auf- und zuklappbare Menügruppen und Menüpunkte. Die Menügruppen enthalten situationsabhängig unterschiedliche Menüpunkte. Nach Anklicken eines Menüpunktes wird die zugehörige Seite im Arbeitsbereich dargestellt.
- Arbeitsbereich (3)
  Im Arbeitsbereich führen Sie die Administrationsaufgaben im Detail durch. Der Arbeitsbereich öffnet sich in der Regel in einem eigenen Fenster. Anzahl und Auswahl der angezeigten Informationen und Aktionen hängen ab vom gewählten Menüpunkt im Navigationsbaum. Im Experten-Modus wird im Arbeitsbereich links der Menübaum angezeigt.

Navigation im Menübaum

Der Menübaum dient zur Navigation im Experten-Modus des WBM. Der Menübaum enthält Ordner (z. B. **Wartung**) mit weiteren Elementen (z. B. **Restart / Reload**).

Sie navigieren im Menübaum durch Klick auf den Ordner (wechselweise auf- und zuklappen).

Automatisches Abmelden nach Zeit

Nach 30 Minuten ohne Aktion werden Sie automatisch abgemeldet. Für weitere Aktionen mit dem WBM müssen Sie sich erneut anmelden. Laden Sie nach einer Pause zur Sicherheit die Seite neu, bevor Sie Änderungen durchführen, damit diese nicht wegen automatischem Abmelden verloren gehen.

3.1.3.1 Wie Sie sich am WBM anmelden

Voraussetzungen

- Ihre Anmeldedaten (Benutzername und Passwort) liegen Ihnen vor. Falls nicht, erfragen Sie diese bitte bei Ihrem Administrator.
- TLS 1.0 ist in den Einstellungen Ihres Webbrowsers aktiviert.

Schritt für Schritt

1) Rufen Sie in Ihrem Webbrowser die Anmeldeseite unter folgender Adresse auf: `https://<IP-Adresse Kommunikationssystem>`. Bei Auslieferung ist die IP-Adresse 192.168.1.2.

2) Klicken Sie oben rechts auf das Sprachkürzel und wählen Sie aus dem Menü die Sprache aus, in der die Oberfläche des WBM angezeigt werden soll. Die Anmeldeseite wird in der ausgewählten Sprache angezeigt.

3) Geben Sie im ersten Feld unter **Login** den Benutzernamen ein. "@system" wird beim Verlassen des Feldes automatisch ergänzt.

4) Geben Sie im zweiten Feld unter **Login** Ihr Passwort ein. Berücksichtigen Sie Groß-/Kleinschreibung und den Zustand der Taste **Num**. Das Passwort wird verdeckt durch Sternchen (*) angezeigt.

5) Klicken Sie auf **Anmelden**.

3.1.3.2 Wie Sie sich vom WBM abmelden

Schritt für Schritt

› Klicken Sie oben rechts auf **Abmelden**.

3.1.4 Benutzerverwaltung des WBM

Sie können für das WBM bis zu 16 Administratoren konfigurieren und verwalten. Jedem Administrator ordnen Sie ein Profil zu, das den Umfang seiner Berechtigungen festlegt.

Die Benutzer des WBM werden als Administratoren bezeichnet.

Der standardmäßig vorhandene Administrator ist `administrator@system` mit dem Standardpasswort `administrator` und dem Profil **Advanced**. Bei der ersten Anmeldung muss das Passwort geändert werden. Das Passwort für einen Administrator muss aus mindestens 8 und höchstens 128 Zeichen bestehen, davon mindestens eine Ziffer. Ein Passwort darf außer Buchstaben und Ziffern folgende Zeichen enthalten: !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~

Profile

Das WBM unterstützt vier Profile mit verschiedenen Berechtigungen für Administratoren mit unterschiedlichen technischen Kenntnissen und Aufgaben.

Profil	Berechtigung
Basic keine Kenntnisse im Konfigurieren des Systems	Systeminformationen auf der Startseite Wizard **Tastenprogrammierung** Wizard **Telefonbuch / Kurzwahl** Wizard **Gesprächsdatenerfassung** Wizard **Wartemusik / Ansagen** Wizard **SmartVM** Wizard **Teilnehmername und Freischaltung** Zugriff auf **Lizenzverwaltung > Lizenzinformationen** Zugriff auf **Service-Center > Dokumente** Zugriff auf **Service-Center > Software**
Enhanced geringe Kenntnisse im Konfigurieren des Systems	wie das Profil **Basic**, plus: Zugriff auf **Service-Center > Inventory** Zugriff auf **Service-Center > Restart / Reload** Zugriff auf **Service-Center > Diagnose > Status** Zugriff auf **Service-Center > Diagnose > Event Viewer**
Advanced geschulter Benutzer	wie das Profil **Enhanced**, plus: alle Wizards Zugriff auf **Administratoren** Zugriff auf **Datensicherung** Zugriff auf die komplette **Lizenzverwaltung** Zugriff auf das komplette **Service-Center** Zugriff auf **Networking**
Expert geschulter Service-techniker	wie das Profil **Advanced**, plus: Zugriff auf den **Experten-Modus**

Das Profil **Expert** ist berechtigt Administratoren hinzuzufügen, sowie Benutzernamen und Passwörter anderer Administratoren zu ändern.

INFO: Solange noch kein Administrator mit dem Profil **Expert** existiert, können Administratoren mit dem Profil **Advanced** weitere Administratoren hinzufügen. Sobald ein Administrator mit dem Profil **Expert** existiert, können nur noch Administratoren mit dem Profil **Expert** weitere Administratoren hinzufügen.

3.1.4.1 Wie Sie einen Administrator hinzufügen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet. (Solange noch kein Administrator mit Profil **Expert** existiert.)
- Sie sind am WBM mit dem Profil **Expert** angemeldet. (Sofern bereits ein Administrator mit Profil **Expert** existiert.)

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Administratoren**.
2) Klicken Sie auf **Hinzufügen…**.
3) Geben Sie folgende Daten ein: **Login-Name**, **Vorname**, **Nachname**, **Passwort**, **Passwort wiederholen**.
4) Wählen Sie in der Aufklappliste **Benutzerrolle** das gewünschte Benutzerprofil.
5) Klicken Sie auf **OK & Weiter**.

3.1.4.2 Wie Sie Administratordaten ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Administratoren**.
2) Aktivieren Sie in der **Administratoren-Liste** das Kontrollkästchen des betreffenden Administrators.
3) Klicken Sie auf **Bearbeiten**.
4) Ändern Sie die entsprechenden Daten.
5) Klicken Sie auf **OK & Weiter**.

3.1.4.3 Wie Sie das Administratorpasswort ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Administratoren**.
2) Aktivieren Sie in der **Administratoren-Liste** das Kontrollkästchen des betreffenden Administrators.

3) Klicken Sie auf **Bearbeiten**.

4) Geben Sie im Feld **Passwort** und im Feld **Passwort wiederholen** jeweils das neue Passwort ein.

5) Klicken Sie auf **OK & Weiter**.

3.1.4.4 Wie Sie einen Administrator löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Administratoren**.

2) Aktivieren Sie in der **Administratoren-Liste** das Kontrollkästchen des betreffenden Administrators.

3) Klicken Sie auf **Löschen…**.

3.1.5 Wizards

Wizards ermöglichen die einfache Installation und Konfiguration des Systems. Für einen Kundenadministrator (Profil **Basic**) steht ein ausgewählter Teil der Wizards zur Verfügung, für einen Administrator mit Fachkenntnissen oder einen geschulten Servicetechniker (Profil **Advanced**) hingegen sämtliche Wizards.

Die zur Verfügung stehenden Wizards hängen von der Systemkonfiguration ab (UC Smart oder UC Suite). Wizards können aus mehreren aufeinanderfolgenden Seiten bestehen. OK & Weiter speichert durchgeführte Änderungen und wechselt zur nächsten Seite des Wizards. Mit OK & Weiter gespeicherte Änderungen können nicht verworfen werden. Sofern keine Änderungen gespeichert wurden, beendet **Abbrechen** den Wizard. Das Anklicken des Symbols **X** in der rechten oberen Ecke des Wizard-Fensters beendet den Wizard und behält zuvor mit OK & Weiter gespeicherte Änderungen bei.

3.1.5.1 Wizards – Grundinstallation

Wizards unter **Grundinstallation** unterstützen die einfache Grundinstallation.

Folgende Wizards sind unter **Grundinstallation** verfügbar:

- **Erstinstallation**
  Einmalige Nutzung bei Ersteinrichtung. Länderintialisierung, System IP-Adresse und DHCP-Server.
- **Basisinstallation**
  Grundeinrichtung des Systems mit Teilnehmerdaten, Amtsleitungen, Netzwerkparameter, Internet.

- **Lizenzierung**
  Lizenzen online aktivieren über den Lizenzserver.
- **Vernetzung-Konfiguration**
  Einrichtung des Systems als Teil einer Vernetzung.
- **Power Management**
  Einrichtung und Aktivierung des Power Managements.

3.1.5.2 Wizards – Netzwerk / Internet

Wizards unter **Netzwerk / Internet** unterstützen die einfache Konfiguration des Netzwerks und des Internet-Zugangs.

Folgende Wizards sind unter **Netzwerk / Internet** verfügbar:

- **Netzwerk-Konfiguration**
  Einrichtung von DHCP, IP-Routing und DNS-Server.
- **Internet-Konfiguration**
  Zugangsparameter der Internet-Providerdaten z.B. User-Account und Passwort.
- **VPN-Konfiguration**
  Anbindung von Arbeitsplätzen über das Internet .

3.1.5.3 Wizards – Endgeräte / Teilnehmer

Wizards unter **Endgeräte / Teilnehmer** unterstützen die einfache Konfiguration von Endgeräten.

Folgende Wizards sind unter **Endgeräte / Teilnehmer** verfügbar:

- **IP-Endgeräte**
  Einrichtung systemspezifischer IP- und SIP-Endgeräte, FAX-Rufnummern sowie IP-/Analogadapter.
- **UP0-Endgeräte**
  Einrichtung UP0-Endgeräte, FAX-Rufnummern.
- **Portable Parts (DECT-Endgeräte)**
  Einrichtung DECT Portable Parts-Endgeräte, FAX-Rufnummern.
- **ISDN-Endgeräte**
  Ungespeiste ISDN Anschlüsse für ISDN Karten/Modems und S0-Teilnehmer.
- **Analog-Endgeräte**
  Analoge MFV und CLIP fähige Anschlüsse für Fax und Telefon.
- **Tastenprogrammierung**
  Namens- und Funktionstastenprogrammierung für systemspezifische IP-Endgeräte und UP0-Endgeräte.

3.1.5.4 Wizards – Zentrale Telefonie

Wizards unter **Zentrale Telefonie** unterstützen die einfache Konfiguration zentraler Telefonie-Leistungsmerkmale.

Folgende Wizards sind unter **Zentrale Telefonie** verfügbar:

- **Amtsleitung ISDN / Analog / ITSP**
  Mehrgeräteanschluss (MSN) und Anlagenrufnummer für ISDN-Anschlüsse, sowie Zuweisung von analogen Amts- und ITSP Leitungen.
- **Internet-Telefonie**
  Zugangsparamter des Internet-Telefonie Service Provider (ITSP) z.B. User-Account, Passwort, SIP-Rufnummer.
- **Telefonbuch / Kurzwahl**
  Einrichtung von zentralen Kurzwahlzielen für das Systeminterne Telefonbuch.
- **Gesprächsdatenerfassung**
  Einrichtung von Verbindungsparameter der Gesprächsdatenerfassung für Gebührenapplikationen.
- **Wartemusik / Ansagen**
  Einspielen von neuen Melodien und Ansagen für die Wartemusik und Ansage vor dem Melden.
- **Türsprechstelle**
  Einrichtung von Rufzordnung und Zugriffsberechtigung der Türsprechstelle am analogen Teilnehmeranschluss.
- **SmartVM**
  Einrichtung der UC Smart Sprachbox (SmartVM).

3.1.5.5 Wizards – User-Telefonie

Wizards unter **User-Telefonie** unterstützen die einfache Konfiguration von Leistungsmerkmalen der User-Telefonie.

Folgende Wizards sind unter **User-Telefonie** verfügbar:

- **Berechtigung**
  Einrichtung von Berechtigungsgruppen mit externen Rufnummern, die dem Teilnehmer zugeordnet werden können, z. B. Notruf, erlaubte Rufnummern, verbotene Rufnummern sowie Zuordnung der Berechtigung zur Nachtschaltung.
- **Teilnehmername und Freischaltung**
  Ändern von Teilnehmer- und Gruppennamen sowie Rücksetzen des Codeschlosses für einzelne Teilnehmer.
- **Gruppenruf / Sammelanschluss**
  Einrichtung von kommenden Anrufen für Teilnehmergruppen (parallele, lineare oder zyklischen Rufreihenfolge).
- **Rufweiterschaltung**
  Einrichtung von zentraler systemweiter Teilnehmerrufzuordnung sowie Weiterschaltung nach Zeit und bei Besetzt.

- **Anrufübernahme**
  Einrichtung von Teilnehmern zu einer Gruppe mit der Möglichkeit der gegenseitigen Rufannahme.
- **Teamschaltung**
  Einrichtung von Teilnehmern, die bei kommenden Gesprächen parallel zum Hauptteilnehmer gerufen werden und bei gehender Verbindung dessen Rufnummer verwenden können.
- **Mobiltelefon Integration**
  Einrichtung einer Verknüpfung zwischen einem Mobiltelefon und einem internen Teilnehmer mit dem Ziel der Erreichbarkeit kommend und gehend unter einer Rufnummer (One Number Service).
- **Chef / Sekretär**
  Einrichtung einer Verknüpfung zwischen einem oder mehreren Chef-Telefonen sowie einem oder mehreren Sekretärinnen-Telefon(en) mit dem Ziel der vereinfachten Gesprächsübergabe und Rufumschaltung.
- **Anrufverteilung**
  Einrichtung einer automatischen intelligenter Anrufverteilung auf eine Gruppe mit ausgewählten Teilnehmer.
- **Vermittlungsplatz**
  Einrichtung von Teilnehmern als Vermittlungsplatzrufnummer sowie des Verhaltens bei Besetzt, Falsch-Wahl und Nicht-Melden.
- **Teilnehmer-Profile**
  Teilnehmer einem Profil zuordnen und Profil-Daten importieren/exportieren.

3.1.5.6 Wizards – Sicherheit

Wizards unter **Sicherheit** unterstützen die einfache Konfiguration der Firewall.

Folgende Wizards sind unter **Sicherheit** verfügbar:

- **Firewall**
  Einrichtung von Portfreigabe zur Einschränkung des Internetverkehrs.

3.1.5.7 Wizards – UC Smart (nur mit UC Smart)

Wizards unter **UC Smart** unterstützen die Einrichtung der UC Lösung UC Smart.

Folgende Wizards sind unter **UC Smart** verfügbar:

- **UC Smart**
  Grundeinrichtung und Benutzerkonfiguration für UC Smart.

3.1.5.8 Wizards – UC Suite (nur mit UC Suite)

Wizards unter **UC Suite** unterstützen die Einrichtung der UC Lösung UC Suite.

Folgende Wizards sind unter **UC Suite** verfügbar:

- **Benutzerverzeichnis**
  Konfiguration der Benutzer.
- **Abteilungent**
  Konfiguration von Abteilungen.
- **Gruppen**
  Konfiguration von Voicemail- und Fax-Gruppen.
- **Templates**
  Konfiguration von SMS-Templates.
- **Externes Verzeichnis**
  Manuelles Hinzufügen einzelner Kontakte zum externen Verzeichnis.
- **Externer Anbieter**
  Eingabe der Zugangsdaten des Exchange- oder LDAP-Servers.
- **Contact Center**
  Konfiguration des Contact Centers.
- **Zeitpläne**
  Konfiguration der Zeitpläne.
- **Datei-Upload**
  Hochladen von Audiodateien für Ansagen und Wartemusik.
- **Konferenzschaltung**
  Konfiguration von Konferenzschaltungen.
- **Profile**
  Erstellen von Benutzer-Profilen.
- **Faxkopfzeilen**
  Konfiguration von Faxkopfzeilen.
- **Skin-Einstellungen**
  Verwaltung von Benutzer-Oberflächen.

3.1.6 Service-Center

Das **Service-Center** des WBM bietet verschiedene Wartungsfunktionen, startet den Software-Update und stellt Dokumentation und Software zur Verfügung.

3.1.6.1 Service Center – Dokumente

Dokumente stellt Dokumentationen, CSV-Vorlagen und Links zu weiterführenden Informationen zur Verfügung. Die Dokumentationen können in allen unterstützten Sprachen als PDF aufgerufen werden.

Je nach Systemkonfiguration sind folgende Inhalte verfügbar:

Inhalt	UC Smart	UC Suite
Administratorokumentationen (PDF)	-	x
Bedienungsanleitungen (PDF)	-	x
Links zu weiterführenden Informationen	x	x
CSV-Vorlagen für den Import von Daten für • Teilnehmer • Kurzwahl zentral • Externes Verzeichnis	x	x

3.1.6.2 Service Center – Software

Software stellt die Software für die UC Clients, USB-Treiber und Tools zur Verfügung.

Folgende Inhalte sind verfügbar:

Inhalt	UC Smart	UC Suite
Installationsdateien für die Software der UC Clients	x	x
USB-Treiber	x	x
Tools	x	x
Links für den direkten Zugriff auf die Installationsdateien	-	x

3.1.6.3 Service-Center – Inventory

Inventory gibt einen Überblick über grundlegende Konfigurationsdaten des Systems.

3.1.6.4 Service-Center – Software-Update

Software-Update überprüft, ob ein SW-Update auf dem Webserver verfügbar ist und führt die Aktualisierung durch.

3.1.6.5 Service-Center – Email-Weiterleitung

Email-Weiterleitung ermöglicht den Versand von E-Mails mit Systemmeldungen von UC Suite an den Administrator und den Versand von E-Mails mit angehängten Sprach- oder Faxnachrichten an Teilnehmer.

3.1.6.6 Service-Center – Remote-Zugang

Remote-Zugang ermöglicht die Konfiguration des Zugangs für die ortsunabhängige Administration des Systems.

3.1.6.7 Service-Center – Restart / Reload

Restart/Reload ermöglicht einen Neustart des Systems, wahlweise mit Zurücksetzen auf Werkseinstellungen.

3.1.6.8 Service-Center – Diagnose > Status

Status bietet Statusinformationen über Netzwerk, Teilnehmer, Verbindungsaufbau, ITSP und VPN.

Siehe auch *Inventory-Management*.

3.1.6.9 Service-Center – Diagnose > Event Viewer

Event Viewer protokolliert Systemereignisse.

Siehe auch *Traces*.

3.1.6.10 Service-Center – Diagnose > Trace

Trace bietet Möglichkeiten zur Fehlerprotokollierung.

Siehe auch *Traces*.

3.1.7 Experten-Modus

Der Experten-Modus stellt geschulten Servicetechnikern (Profil **Expert**) Menüs mit Funktionen für die Konfiguration und Wartung des Systems zur Verfügung.

Ausführliche Informationen finden Sie in Kapitel *Experten-Modus*.

3.1.8 Online-Hilfe

Die integrierte Online-Hilfe beschreibt wichtige Konzepte und Handlungsanweisungen. Zu jeder geöffneten WBM-Seite wird kontextsensitiv das zugehörige Hilfe-Thema aufgerufen.

Navigation

Die Schaltflächen in der Online-Hilfe bieten folgende Funktionen:

- **Inhalt**
  gibt einen Überblick über die Struktur
- **Index**
  bietet direkten Zugang zu einem Thema über Stichworte
- **Suchen**
  bietet eine Volltextsuche zum gezielten Auffinden relevanter Themen

3.1.8.1 Wie Sie die Online-Hilfe kontextsensitiv aufrufen

Voraussetzungen

- Sie sind am WBM angemeldet.

Schritt für Schritt

› Klicken Sie im geöffneten WBM-Fenster entweder auf das Fragezeichensymbol rechts oben oder auf die Hilfe-Schaltfläche links unten.

3.2 Manager E

Manager E ist ein Servicetool mit integrierter Hilfe unter Windows für Tasks, die nicht im WBM durchführbar sind.

Der Manager E kann verwendet werden für die OpenScape Business X3, OpenScape Business X5 und OpenScape Business X8. Die OpenScape Business X1 ist nicht mit dem Manager E administrierbar (einzige Ausnahme: die Konfiguration des Online-Users).

Manager E ist für geschultes Servicepersonal bestimmt und beinhaltet folgende Funktionsblöcke:

- Generierung (auch Offline-Generierung)
- Kundendatenabzug und -sicherung
- Serviceaufträge wie z. B. Neustart von Baugruppen
- Rücksetzen von aktivierten Leistungsmerkmalen
- Erstellung und Ausdruck von:
  - Tastenbeschriftungen für optiPoint 500
  - Kundendatenlisten
  - Hauptverteilerbelegungen
- eigene Nutzer- und Passwortverwaltung für den Service
- Konvertierungsroutine für Kundendatenspeicher

Der Systemzugang über Manager E erfolgt mit einem eigenen Benutzernamen und Passwort. Um kleinere Änderungen schnell durchzuführen steht der Online-Mode zur Verfügung. Die Funktionalität des Online-Mode entspricht der Bedienoberfäche von Assistant T.

Folgende Leistungsmerkmale sind nicht mehr über Manager E administrierbar:

- Lizenzierung
- Netzwerk
  - SNMP-Partner
  - PSTN-Partner
  - Routing
  - Mapping
  - Gatekeeper
  - Ext. H.323
  - IP-Ports
- Maintenance
  - Error History
  - Event Log
  - Tracereinstellungen
  - Error Reaction Table
  - V.24 Status
  - DMA
- Traces

Arbeitsweise mit dem Kundendatenspeicher (KDS)

Die grundsätzliche Arbeitsweise läuft in folgenden Schritten ab:

- KDS vom System in Manager E laden
- Änderungen in Manager E durchführen
- KDS von Manager E in das System sichern

3.2.1 Wie Sie den KDS in den Manager E laden

Führen Sie die folgenden Schritte durch um anschließend Konfigurationsaufgaben in Manager E durchzuführen.

Schritt für Schritt

1) Starten Sie Manager E am Admin-PC.

2) Geben Sie **Benutzername** für Manager E ein.

3) Geben Sie das **Kennwort** für Manager E ein.

4) Klicken Sie auf **Datei > Übertragen**.

5) Klicken Sie auf die Registerkarte **Kommunikation**.

6) Aktivieren Sie im Bereich **Zugang** die entsprechende Option, je nach Verbindungsart des Admin-PC zum System.

7) Aktivieren Sie die Option **KDS lesen/schreiben**.

8) Klicken Sie auf **Anlage -> PC**.

9) Klicken Sie auf **OK**. Der KDS wird vom System zu Manager E übertragen.

10) Klicken Sie nach erfolgreicher Übertragung auf **OK**.

11) Klicken Sie auf **Schließen**.

3.2.2 Wie Sie den KDS in das System zurücksichern

Führen Sie die folgenden Schritte durch um im Manager E durchgeführte Konfigurationen in das System zurück zu sichern.

Schritt für Schritt

1) Klicken Sie auf **Datei > Übertragen**.

2) Klicken Sie auf die Registerkarte **Kommunikation**.

3) Aktivieren Sie im Bereich **Zugang** die entsprechende Option, je nach Verbindungsart des Admin-PC zum System.

4) Aktivieren Sie die Option **KDS lesen/schreiben**.

5) Klicken Sie auf **PC -> Anlage**.

6) Klicken Sie auf **OK**. Der KDS wird von Manager E zum Sytem übertragen.

7) Klicken Sie nach erfolgreicher Übertragung auf **OK**.

8) Klicken Sie auf **Schließen**.

4 Erstinstallation OpenScape Business X

Beschrieben wird die Erstinstallation von OpenScape Business X1/X3/X5/X8. Das Kommunikationssystem und die zugehörenden Komponenten werden in eine vorhandene Infrastruktur integriert bestehend aus einem Kunden-LAN und einem TDM-Telefonienetz. Es werden der Internet-Zugang und der Amtsanschluss eingerichtet und die angeschlossenen Teilnehmer konfiguriert.

Die Erstinstallation von OpenScape Business X1/X3/X5/X8 (kurz Kommunikationssystem genannt) wird mit dem Administrationsprogramm OpenScape Business Assistant (Web-based Management, kurz WBM genannt) durchgeführt.

Beschrieben wird die Standard-Erstinstallation häufig verwendeter Komponenten. Die Installationssschritte sind abhängig vom Kommunikationssystem und den Komponenten (z. B. UC Booster Card). Eventuell müssen Sie bei der Erstinstallation an einigen Stellen zwischen mehreren Möglichkeiten wählen oder Konfigurationen sogar ganz überspringen. Es ist auch möglich, dass hier beschriebene Installationssschritte bei Ihrem Kommunikationssystem nicht erscheinen.

Die ausführliche Konfiguration der über die Standard-Erstinstallation hinausgehenden Leistungsmerkmale finden Sie in den anschließenden Kapiteln.

Voraussetzung für die Erstinstallation ist die Erstellung eines IP-Adress-Schemas und eines Rufnummernplans.

Die wichtigsten Installationsschritte:

- IP-Adressen- und DHCP-Einstellungen
- Länder- und Zeiteinstellungen
- Systemrufnummern und Vernetzung
- ISDN-Konfiguration
- Internet-Zugang
- Internet-Telefonie
- Teilnehmer-Konfiguration
- Lizenzierung
- Datensicherung

4.1 Voraussetzungen für die Erstinstallation

Die Erfüllung der Voraussetzungen für die Erstinstallation gewährleistet den Betrieb des Kommunikationssystems.

Allgemein

Abhängig von der verwendeten Hardware (Baugruppen, Telefone,...) und der vorhandenen Infrastruktur gelten folgende allgemeine Voraussetzungen:

- Die Infrastruktur (LAN, TDM-Telefonienetz) ist vorhanden und nutzbar.
- Die Hardware ist korrekt montiert und angeschlossen.

- Für die Intergration des Mainboards und der UC Booster Card ins Kunden-LAN wird jeweils eine LAN-Schnittstelle benötigt.
- Das Kommunikationssystem ist noch nicht ans LAN angeschlossen.
- Wird die UC Booster Card verwendet, sollte es vor der Erstinstallation gesteckt werden.
- Ein Internet-Zugang bei einem Internet-Service-Provider ist vorhanden.
- Für die Nutzung eines ISDN-Amtszugangs ist ein ISDN-S_0- oder ein ISDN-Primärmultiplexanschluss nötig.
- Für die Nutzung eines CAS-Amtszugangs ist ein CAS-Amtsanschluss nötig.
- Für die Nutzung eines analogen Amtszugangs ist ein analoger Amtsanschluss nötig.
- Ein IP-Adressen-Schema ist vorhanden und bekannt (siehe *IP-Adressen-Schema*).
- Ein Rufnummernplan ist vorhanden und bekannt (siehe *Rufnummernplan*).

Admin-PC

Für den Administrations-PC (Admin-PC), mit dem die Erstinstallation und die spätere Administration des Kommunikationssystems durchgeführt wird, sind folgende Voraussetzungen nötig:

- Netzwerk-Schnittstelle:
  Der Admin-PC benötigt eine freie LAN-Schnittstelle.
- Betriebssystem:
  Für eine evtl. Konfiguration des Kommunikationssystems mit dem Manager E ist ein Windows-Betriebssystem (ab Windows XP) Voraussetzung.
  Die Konfiguration mit dem WBM ist browserbasiert und somit betriebssystemunabhängig.
- Webbrowser:
  Es werden die nachfolgenden Webbrowser unterstützt:
  - Microsoft Internet Explorer ab Version 10.
  - Mozilla Firefox ab Version 17.

  Falls eine ältere Webbrowser-Version installiert ist, muss eine aktuelle Version installiert werden, bevor mit der Erstinbetriebnahme begonnen werden kann.
- Java Runtime Environment:
  Es muss immer die aktuellste Version des Java Runtime Environments installiert sein. Ist eine ältere Version installiert, muss auf die aktuellste Version aktualisiert werden, bevor mit der Erstinbetriebnahme begonnen werden kann.

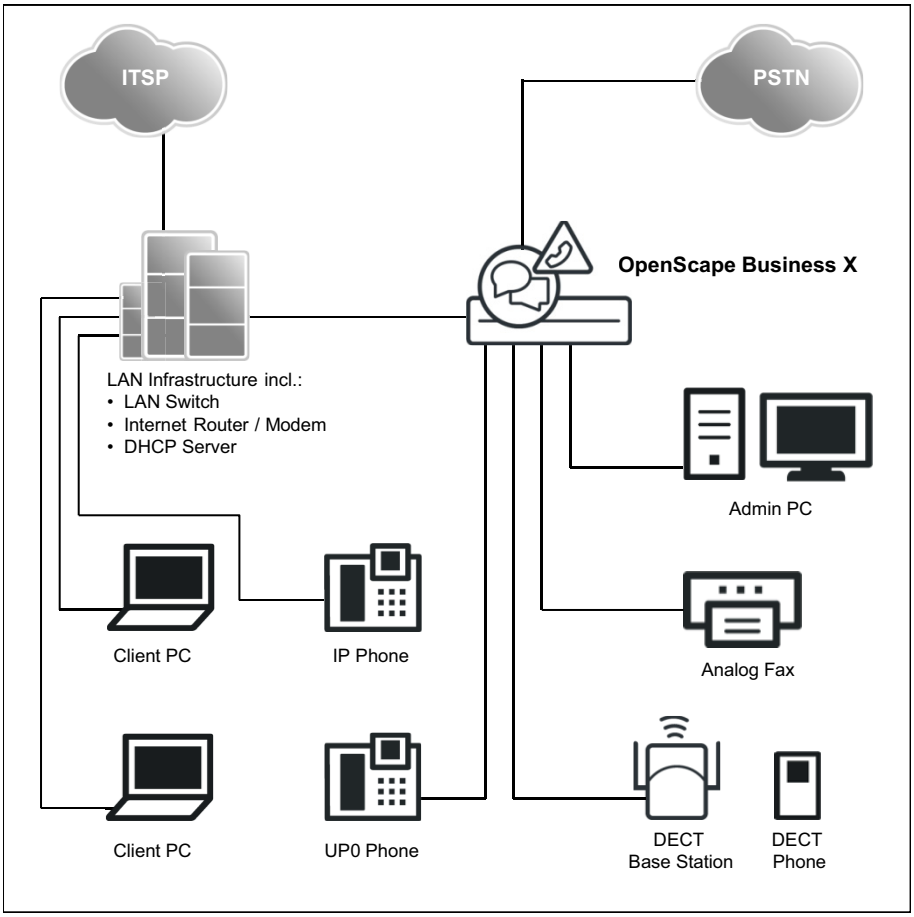
4.2 Komponenten

Die Komponenten des Installationsbeispiels sind im Folgenden beschrieben und skizziert.

Das Installationsbeispiel umfasst folgende Komponenten:

- OpenScape Business X
  Das Kommunikationssystem wird über die LAN-Schnittstelle in das vorhandene Kunden-LAN eingebunden
- Admin-PC
  Der Admin-PC wird ebenfalls über eine LAN-Schnittstelle mit dem Kommunikationssystem verbunden.
- IP-Teilnehmer (IP-Clients)
  Die IP-Teilnehmer (IP-Systemtelefone, Client-PCs, WLAN Access Points, ...) sind über einen oder mehrere Switches im LAN integriert.
- UP0-Teilnehmer
  Die UP0-Teilnehmer (z. B. TDM-Systemtelefon OpenStage 60T) sind direkt am Kommunikationssystem angeschlossen.
- Analoge Teilnehmer
  Die analogen Teilnehmer (z. B. analoges FAX) sind direkt am Kommunikationssystem angeschlossen.
- DECT-Teilnehmer
  Die DECT-Teilnehmer sind über eine Basisstation am Kommunikationssystem angemeldet.

Die IP-Clients erhalten ihre IP-Adressen dynamisch von einem internen oder externen DHCP-Server (z. B. Internet-Router).



4.3 Rufnummernplan

Ein Rufnummernplan ist eine Liste aller im Kommunikationssystem verfügbaren Rufnummern. Er beinhaltet u.a. interne Rufnummern, Durchwahlnummern und Gruppenrufnummern.

Standard-Rufnummernplan

Die internen Rufnummern sind mit Standardwerten vorbelegt. Diese Werte können bei Bedarf an die eigenen Belange angepasst werden (individueller Rufnummernplan).

Auszug aus dem Standard-Rufnummernplan:

Art der Rufnummern	X1	X3/X5/X8
Interne Teilnehmer-Rufnummern	11-30	100-742
Teilnehmer-Durchwahlnummern	11-30	100-742
Leitungsrufnummern	700-703	ab 7801

Art der Rufnummern	X1	X3/X5/X8
Richtungskennzahlen (Externkennzahlen):		
Rtg. 1 (Amt ISDN, analog)	0 = Welt / 9 = USA	0 = Welt / 9 = USA
Rtg. 8 (UC Suite)	-	851
Rtg. 12-15 (Amt ITSP)	nicht vorbelegt	855-858
Rtg. 16 (Vernetzung)	nicht vorbelegt	859
Rufnummer für den Remote-Zugang	nicht vorbelegt	nicht vorbelegt
Rufnummer für Sprachnachrichten		
UC Smart	351	351
UC Suite	-	nicht vorbelegt

Individueller Rufnummernplan

Ein individueller Rufnummernplan kann während der Basiskonfiguration über eine XML-Datei importiert werden.

Die XML-Datei enthält mehrere Register. Das Register "Stations" enthält zusätzlich zu den Namen und den Rufnummern der Teilnehmer weitere Teilnehmerdaten, wie z. B. die Teilnehmer-Typen und die E-Mail-Adressen der Teilnehmer.

Ein Beispiel einer XML-Datei mit zugehöriger Erklärung finden Sie im WBM unter **Service-Center > Dokumente > CSV-Vorlagen**. Die dort abgelegte XML-Datei können Sie auch als Vorlage für Ihre Daten verwenden. Sie kann z. B. mit Microsoft Excel bearbeitet werden.

4.4 IP-Adressen-Schema

Ein IP-Adressen-Schema ist eine Festlegung, wie die IP-Adressen im Kunden-LAN vergeben sind. Es beinhaltet die IP-Adressen von PCs, Servern, Internet-Routern, IP-Telefonen, dem Kommunikationssystem, usw.

Für eine bessere Übersicht bei der Zuordnung von IP-Adressen sollte ein IP-Adressen-Schema erstellt werden.

Beispiel eines IP-Adressen-Schemas mit dem IP-Adressband `192.168.1.x`:

IP-Adressbereich	Clients
192.168.1.1 bis **192.168.1.19**	Clients mit fester IP-Adresse:
192.168.1.1	Internet-Router (Gateway)
192.168.1.2	Kommunikationssystem

IP-Adressbereich	Clients
192.168.1.3	Application Board (optional)
192.168.1.10	E-Mail-Server
192.168.1.50 bis **192.168.1.254**	Client-PCs & IP-Telefone, zugleich IP-Adressband des DHCP-Servers, Zuweisung der IP-Adressen an die Clients erfolgt dynamisch

Folgende IP-Adressbereiche sind intern reserviert und dürfen nicht belegt sein:

ausgeschlossene IP-Adressbereiche	Beschreibung
10.0.0.1; 10.0.0.2	reserviert für Lizenzserver
10.186.237.65; 10.186.237.66	reserviert für Remote ISDN
192.168.3.2	Interne IP-Adresse des Kommunikationssystems
192.168.2.1	IP-Adresse der LAN3-Schnittstelle (Admin-Port)

Diese Liste finden Sie auch im WBM unter **Service-Center > Diagnose > Status > Übersicht IP-Adressen**.

Erweiterung der Netzmaske bei Verwendung des voreingestellten Netzsegments

Sowohl die interne IP-Adresse des Kommunikationssystems als auch die IP-Adresse der LAN3-Schnittstelle (Admin-Port) dürfen nicht im gleichen Netzsegment liegen wie die IP-Adresse der Kommunikationssystems.

Voreingestellte Netzsegment-Konfiguration:

- 192.168.1.2: IP-Adresse des Kommunikationssystems
- 255.255.255.0: Netzmaske
- 192.168.3.2: interne IP-Adresse des Kommunikationssystems
- 192.168.2.1: IP-Adresse der LAN3-Schnittstelle (Admin-Port)

Wird die Netzmaske bei Verwendung des voreingestellten Netzsegments von 255.255.255.0 auf z. B. 255.255.0.0 erweitert, müssen die o.g. IP-Adressen geändert werden:

Beispiel einer geänderten Konfiguration:

- 192.168.1.2: IP-Adresse des Kommunikationssystems
- 255.255.**0**.0: Netzmaske
- 192.**169**.3.2: interne IP-Adresse des Kommunikationssystems
  Änderbar über **Experten-Modus > Telefonie > Payload > HW-Module > DSP-Einstellungen ändern**
- 192.**170**.2.1: IP-Adresse der LAN3-Schnittstelle (Admin-Port)
  Änderbar über **Experten-Modus > Telefonie > Netzwerkschnittstellen > Mainboard > LAN 3 (Admin)**

4.5 Erstinbetriebnahme

Die Erstinbetriebnahme umfasst den Start des Kommunikationssystems, den Anschluss und die Konfiguration des Admin-PCs und das erstmalige Starten des Administrationsprogramms OpenScape Business Assistant (WBM).

Die Erstinbetriebnahme des Kommunikationssystems muss durchgeführt werden, bevor das Kommunikationssystem in das interne LAN integriert wird. Es kann zu Problemen kommen, wenn die vorkonfigurierte IP-Adresse des Kommunikationssystems schon im internen LAN vorhanden ist und/oder bereits ein DHCP-Server genutzt wird. Für diese Fälle muss zuerst die IP-Adresse des Kommunikationssystems umkonfiguriert werden und/oder der DHCP-Server des Kommunikationssystems deaktiviert werden. Erst dann kann das Kommunikationssystems ins interne LAN integriert werden.

INFO: Vor der Erstinbetriebnahme sind die Hinweise zum Datenschutz und zur Datensicherheit zu beachten.



GEFAHR

Das Einschalten von OpenScape Business X8 darf erst erfolgen, wenn die Rückseite aller Systemboxen mit den dafür vorgesehenen Anschluss- und Blind-Panels verschlossen ist.



GEFAHR

Das Einschalten von OpenScape Business X3R/X5R darf nur mit geschlossener Gehäusefront erfolgen. Nicht mit Baugruppen bestückte Steckplätze sind immer mit Leerblenden (C39165-A7027-B115) zu verschließen.



GEFAHR

Das Einschalten von OpenScape Business X1/X3W/X5W darf nur bei geschlossenem Gehäuse erfolgen.

Anschluss des Admin-PCs

Um das Kommunikationssystem zu konfigurieren, wird der Admin-PC direkt an die LAN-Schnittstelle "LAN" des Kommunikationssystems angeschlossen und so konfiguriert, dass er seine IP-Adresse vom internen DHCP-Server des Kommunikationssystems bezieht. Nach erfolgreicher Installation kann der Admin-PC ohne weitere Konfigurationsänderungen ins interne LAN integriert werden.

4.5.1 Wie Sie das Kommunikationssystem starten

Voraussetzungen

- Die Montage der Hardware wurde ordnungsgemäß durchgeführt (siehe OpenScape Business V1, Montage der Hardware).
- Die Speicherkarte (mit der System-Software) ist gesteckt.
- Das Kommunikationssystem ist noch nicht in das Kunden-LAN integriert.

Schritt für Schritt

› Verbinden Sie das Kommunikationssystem mit dem Stromnetz.



WARNUNG

Elektrischer Schlag durch Berühren spannungsführender Leitungen

Achten Sie darauf, dass das Kommunikationssystem (und bei OpenScape Business X8 jede Systembox) durch einen separaten Schutzleiter geerdet ist (siehe OpenScape Business V1, Montage der Hardware).

Das Kommunikationssystem wird jetzt hochgefahren. Dabei leuchten die LEDs des Systems in unterschiedlichen Farben und Sequenzen (Details siehe OpenScape Business V1, Montage der Hardware). Während des Hochfahrens darf das Kommunikationssystem nicht vom Stromnetz getrennt werden.

Nach Abschluss des Hochfahrens blinkt die LED "Run" des Mainboards grün im 1Hz-Takt (0,5s an / 0,5s aus).

4.5.2 Wie Sie den Admin-PC mit dem Kommunikationssystem verbinden

Voraussetzungen

- Das Kommunikationssystem ist betriebsbereit.

Schritt für Schritt

1) Starten Sie den Admin-PC.

2) Kontrollieren Sie, ob dem PC eine dynamische IP-Adresse zugewiesen werden kann. Falls nicht, müssen Sie den Admin-PC umkonfigurieren. Dafür benötigen Sie Administratorrechte.

INFO: Die hier beschriebenen IP-Einstellungen gelten für Windows 7. Ausführliche Informationen zur Einrichtung bei

anderen Windows-Betriebssystemen entnehmen Sie bitte der jeweiligen Betriebssystemanleitung.

a) Wählen Sie **Start > Systemsteuerung** und doppelklicken Sie auf **Netzwerk und Internet** und anschließend auf **Netzwerk- und Freigabe-center**.

b) Klicken Sie bei dem entsprechenden aktiven Netzwerk auf **LAN-Verbindung** und anschließend auf **Eigenschaften**.

c) Markieren Sie in der Registerkarte **Netzwerk** mit der linken Maustaste den Eintrag **Internetprotokoll Version 4 (TCP/IPv4)** und klicken Sie auf **Eigenschaften**.

d) Klicken Sie auf die Registerkarte **Allgemein** und kontrollieren Sie, ob das Optionsfeld **IP-Adresse automatisch beziehen** aktiviert ist. Falls nicht, aktivieren Sie es.

e) Schließen Sie alle geöffneten Fenster mit **OK**.

3) Verbinden Sie über ein LAN-Kabel die soeben konfigurierte LAN-Schnittstelle des Admin-PC mit der LAN-Schnittstelle "LAN" des Kommunikationssystems. Über diese Schnittstelle wird dem Admin-PC eine dynamische IP-Adresse zugewiesen.

INFO: Sie können den Admin-PC auch an die LAN-Schnittstelle "Admin" anschließen, dann müssen Sie allerdings dem Admin-PC eine feste IP-Adresse aus dem Bereich 192.168.2.xxx (z. B. 192.168.2.40) und die Netzmaske 255.255.255.0 vergeben. Das Kommunikationssystem hat über die LAN-Schnittstelle "Admin" die IP-Adresse 192.168.2.1 - wichtig für WBM-Zugang!

4.5.3 Wie Sie das WBM starten

Voraussetzungen

- Das Kommunikationssystem ist betriebsbereit. Die LED "Run" des Mainboards blinkt grün im 1Hz-Takt (0,5s an / 0,5s aus).
- Admin-PC und Kommunikationssystem können über LAN miteinander kommunizieren.

Schritt für Schritt

1) Starten Sie auf dem Admin-PC den Webbrowser und rufen Sie die Anmeldeseite von OpenScape Business Assistant (WBM) unter folgender Adresse auf:

```
https://192.168.1.2
```

INFO: Lässt sich das WBM nicht starten, prüfen Sie die LAN-Verbindung und wiederholen Sie den Aufruf. Lässt es sich noch

immer nicht starten, prüfen Sie, ob die IP-Adresse durch Ihre PC-interne Firewall geblockt wird. Genauere Informationen finden Sie in der Dokumentation Ihrer Firewall.

2) Wenn der Webbrowser ein Problem mit einem Sicherheitszertifikat meldet, installieren Sie das Zertifikat (am Beispiel der Internet Explorers V10).

a) Schließen Sie den Webbrowser.

b) Öffnen Sie den Webbrowser mit Administratorrechten, indem Sie mit der rechten Maustaste auf das Webbrowser-Symbol klicken und im Kontextmenü den Eintrag **Als Administrator ausführen** auswählen.

c) Erlauben Sie die Benutzerkontensteuerung.

d) Rufen Sie die Anmeldeseite von OpenScape Business Assistant (WBM) unter folgender Adresse auf:

`https://192.168.1.2`

e) Klicken Sie auf **Laden dieser Website fortsetzen**.

f) Klicken Sie auf die Meldung **Zertifikatsfehler** in der Navigationsleiste des Webbrowsers.

g) Klicken Sie auf **Zertifikate anzeigen**.

h) Klicken Sie auf **Zertifikat installieren** (nur sichtbar mit Administratorrechten).

i) Wählen Sie die Option **Lokaler Computer** und bestätigen Sie mit **Weiter**.

j) Wählen Sie die Option **Alle Zertifikate in folgendem Speicher speichern**, klicken Sie auf **Durchsuchen** und geben Sie **Vertrauenswürdige Stammzertifizierungsstellen** an.

k) Bestätigen Sie mit **OK** und anschließend mit **Weiter** und **Fertigstellen**.

l) Bestätigen Sie den Zertifikatimport mit **OK** und schließen Sie das Zertifikatsfenster mit **OK**.

m) Schließen Sie den Webbrowser.

n) Starten Sie den Webbrowser erneut (ohne Administratorrechte) und rufen Sie die Anmeldeseite von OpenScape Business Assistant (WBM) unter folgender Adresse auf:

`https://192.168.1.2`

3) Klicken Sie oben rechts auf das Sprachkürzel und wählen Sie aus dem Menü die Sprache aus, in der die Oberfläche des WBM angezeigt werden soll. Die Anmeldeseite wird in der ausgewählten Sprache angezeigt.

4) Geben Sie im ersten Feld unter **Login** den Standard-Benutzernamen `administrator@system` für den Zugang als Administrator ein.

INFO: Wenn Sie nach Eingabe von `administrator` in das Feld **Passwort** wechseln, wird `@system` automatisch ergänzt.

5) Geben Sie im zweiten Feld unter **Login** das Standard-Passwort `administrator` für den Zugang als Administrator ein.

6) Klicken Sie auf **Login**.

7) Folgende Schritte sind nur einmalig beim ersten Anmelden am WBM nötig:

a) Geben Sie im Feld **Passwort** nochmal das Standard-Passwort `administrator` ein.

b) Geben Sie in den Feldern **Neues Passwort** und **Neues Passwort bestätigen** ein neues Passwort ein, um das System gegen Missbrauch zu schützen. Berücksichtigen Sie Groß-/Kleinschreibung und den Zustand der Tasten `Num` und `CapsLock` (Feststelltaste). Das Passwort erscheint verdeckt durch Sternchen (*).

INFO: Das Passwort muss mindestens 8 Zeichen lang sein und eine Ziffer enthalten. Bitte merken Sie sich Ihr neues Passwort genau.

---

c) Klicken Sie auf **Login**.

d) Wählen Sie das aktuelle Datum aus und tragen Sie die Uhrzeit korrekt ein.

e) Klicken Sie auf **OK & Weiter**. Sie werden automatisch vom WBM abgemeldet.

f) Geben Sie im ersten Feld unter **Login** den Standard-Benutzernamen `administrator@system` für den Zugang als Administrator ein.

INFO: Wenn Sie nach Eingabe von `administrator` in das Feld **Passwort** wechseln, wird `@system` automatisch ergänzt.

---

g) Geben Sie im zweiten Feld unter **Login** Ihr neu definiertes Passwort für den Zugang als Administrator ein.

h) Klicken Sie auf **Login**. Es erscheint die Startseite des WBM.

Nächste Schritte

Erstinstallation starten.

4.6 Integration ins Kunden-LAN

Die Integration ins Kunden-LAN wird mit dem Wizard **Erstinstallation** des WBM durchgeführt. Dabei werden die grundlegenden Einstellungen für die Einbindung des Kommunikationssystems in das bestehende LAN festgelegt.

4.6.1 Wie Sie den Wizard Erstinstallation starten

Voraussetzungen

- Das WBM ist gestartet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie auf **Bearbeiten**, um den Wizard **Erstinstallation** zu starten.

> ***INFO:*** Wenn bei niedrigen Bildschirmauflösungen der Arbeitsbereich aufgrund der Größe des Browserfensters nicht komplett angezeigt werden kann, so erscheinen horizontale oder vertikale Rollbalken an den Rändern, mit denen der angezeigte Ausschnitt verschoben werden kann.

Nächste Schritte

Führen Sie die Erstinstallation wie nachstehend beschrieben Schritt für Schritt durch. Felder, die hier nicht beschrieben werden, sind passend für den Standardfall vorbelegt und müssen nur geändert werden, wenn sie nicht zu Ihren Netzwerkdaten passen. Die ausführlichen Informationen finden Sie in der Administratordokumentation bei der Beschreibung der einzelnen Wizards.

4.6.2 Systemeinstellungen

Im Fenster **Systemeinstellungen** konfigurieren Sie die Systemeinstellungen des Kommunikationssystems.

Gehen Sie folgendermaßen vor:

1. Display-Logo und Produktbezeichnung festlegen
   Sie können einen Display-Text festlegen, das im Display der Systemtelefone angezeigt wird. Zusätzlich können Sie die Produktbezeichnung auswählen.
2. IP-Adressen festlegen (falls nötig)
   Dem Kommunikationssystem ist standardmäßig eine IP-Adresse und eine Subnetzmaske zugewiesen. Eventuell müssen Sie IP-Adresse und/oder Subnetzmaske an Ihren eigenen IP-Adressbereich anpassen.
   Zusätzlich können Sie die IP-Adresse Ihres Default-Routers angeben, z. B. die IP-Adresse des Internet-Routers.
   Das Application Board (UC Booster Card) benötigt ebenfalls eine IP-Adresse. Sie können unabhängig davon, ob es montiert ist oder nicht, eine IP-Adresse aus Ihrem IP-Adressbereich vergeben.

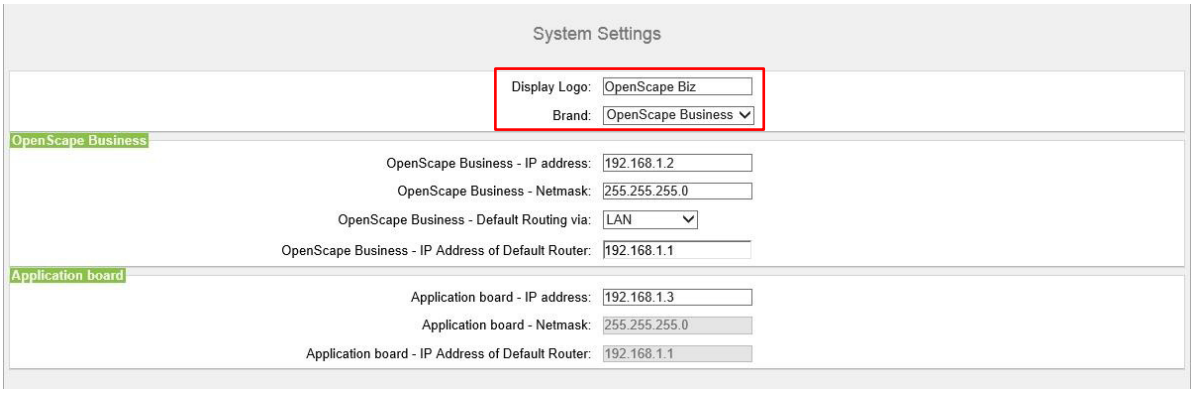
Soll die Netzmaske erweitert werden, z.B. von 255.255.255.0 auf 255.255.0.0, müssen sowohl die interne IP-Adresse des Kommunikationssystems als auch die IP-Adresse der LAN3-Schnittstelle (Admin-Port) geändert werden, da diese nicht

im gleichen Netzsegment liegen dürfen wie die IP-Adresse der Kommunikationssystems (siehe auch *IP-Adressen-Schema*).

4.6.2.1 Wie Sie das Display-Logo und die Produktbezeichnung festlegen

Voraussetzungen

- Sie befinden sich im Fenster **Systemeinstellungen**.



Schritt für Schritt

1) Geben Sie im Feld **Display-Logo** einen Text Ihrer Wahl ein (z. B. OpenScape Biz). Der Text kann bis zu 16 Zeichen lang sein. Vermeiden Sie Umlaute und Sonderzeichen.

2) Wählen Sie in der Aufklappliste **Produkt** die Produktbezeichnung aus.

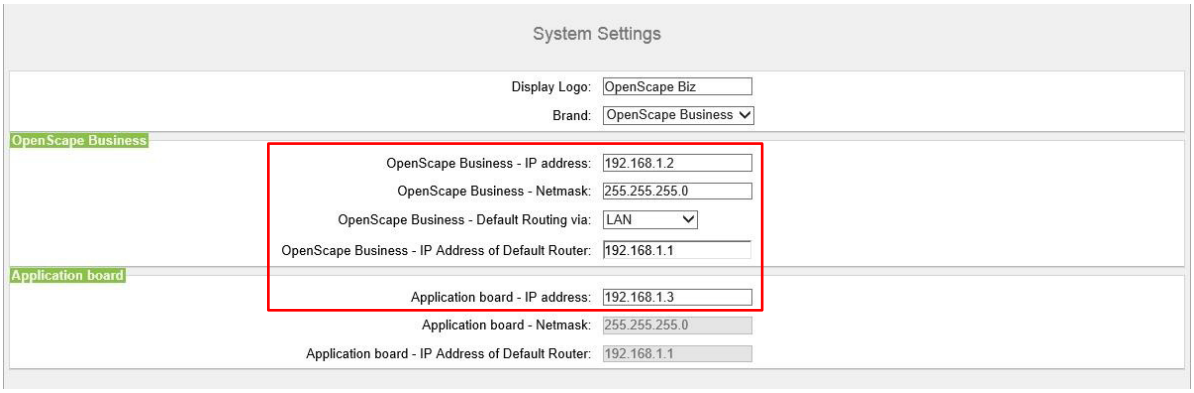
Nächste Schritte

IP-Adressen ändern (falls nötig) oder DHCP konfigurieren.

4.6.2.2 Wie Sie die IP-Adressen festlegen (optional)

Voraussetzungen

- Ihnen ist der IP-Adressbereich Ihres internen Netzes bekannt.
- Sie befinden sich im Fenster **Systemeinstellungen**.



Schritt für Schritt

1) IP-Adresse des Kommunikationssystems festlegen:

a) Geben Sie im Feld **OpenScape Business - IP-Adresse** eine IP-Adresse ein, die im IP-Adressbereich Ihres internen Netzes liegt (z. B. internes Netz: `192.168.1.x`, OpenScape Business: `192.168.1.2`).

INFO: Die IP-Adresse für OpenScape Business darf keinem weiteren Netzwerk-Client zugewiesen sein, da es sonst zu einem IP-Adressenkonflikt kommt.

---

b) Geben Sie im Feld **OpenScape Business - Netzmaske** die Netzmaske Ihres internen Netzes an (z. B. `255.255.255.0`).

2) IP-Adresse des Default-Routers festlegen:

a) Wählen Sie im Feld **OpenScape Business - Default Routing über** den Eintrag **LAN** aus.

b) Geben Sie im Feld **OpenScape Business - IP-Adresse des Default-Routers** die IP-Adresse Ihres Default-Routers an (z. B. internes Netz: `192.168.1.x`, Internet-Router als Default-Router: `192.168.1.1`).

3) IP-Adresse der UC Booster Card festlegen (nötig, wenn gesteckt):

a) Geben Sie im Feld **UC Booster Card - IP-Adresse** eine IP-Adresse ein, die im IP-Adressbereich Ihres internen Netzes liegt (z. B. internes Netz: `192.168.1.x`, UC Booster Card: `192.168.1.3`).

INFO: Die IP-Adresse der UC Booster Card darf keinem weiteren Netzwerk-Client zugewiesen sein, da es sonst zu einem IP-Adressenkonflikt kommt.

---

4) Klicken Sie auf **OK & Weiter**.

Nächste Schritte

DHCP konfigurieren.

4.6.3 DHCP-Einstellungen

Im Fenster **DHCP globale Einstellungen** aktivieren und konfigurieren oder deaktivieren Sie den internen DHCP-Server des Kommunikationssystems.

Ein DHCP-Server weist den IP-Teilnehmern (IP-Systemtelefone, PCs, usw.) automatisch eine IP-Adresse zu und versorgt sie mit netzwerkspezifischen Daten, wie z. B. der IP-Adresse des Standard-Gateways (Internet-Router).

Als DHCP-Server kann ein externer DHCP-Server genutzt werden (z. B. der DHCP-Server des Internet-Routers) oder der interne DHCP-Server, der im Kommunikationssystem integriert ist.

Für die automatische Softwareaktualisierung der IP-Systemtelefone kann der im Kommunikationssystem integrierte DLI oder ein externer DLS-Server verwendet werden (*Deployment Service (DLI und DLS)*). Dem DHCP-Server muss die IP-Adresse des integrierten DLI oder des externen DLS-Servers bekannt sein.

Sie haben folgende Möglichkeiten:

- Internen DHCP-Server aktivieren und konfigurieren
  Wird der interne DHCP-Server des Kommunikationssystems verwendet, muss ein externer DHCP-Server (z. B. der DHCP-Server des Internet-Routers) deaktiviert werden. Eventuell müssen die Einstellungen des internen DHCP-Servers an das Kunden-LAN angepasst werden. Wird der interne DHCP-Server und der interne DLI genutzt, werden die Systemtelefone automatisch aktualisiert. Wird ein externer DLS-Server genutzt, muss seine IP-Adresse im internen DHCP-Server über den Experten-Modus eingetragen werden (*Deployment Service (DLI und DLS)*).
- Internen DHCP-Server deaktivieren
  Wird ein externer DHCP-Server genutzt, muss der interne DHCP-Server des Kommunikationssystems deaktiviert werden. Damit die IP-Systemtelefone automatisch mit der aktuellsten Telefonsoftware versorgt werden, müssen im externen DHCP-Server die netzwerkspezifischen Daten eingegeben werden, wie z. B. die IP-Adresse des internen DLI oder des externen DLS-Servers.

> ***INFO:*** Nicht alle externen DHCP-Server unterstützen die Eingabe von netzwerkspezifischen Daten! In diesem Fall müssen die Daten an allen IP-Systemtelefonen manuell eingeben werden.

4.6.3.1 Wie Sie den internen DHCP-Server deaktivieren

Voraussetzungen

- Im internen Netz ist ein externer DHCP-Server (z. B. der DHCP-Server des Internet-Routers) aktiviert.
- Sie befinden sich im Fenster **DHCP globale Einstellungen**.

Schritt für Schritt

1) Deaktivieren Sie das Kontrollkästchen **DCHP-Server aktivieren**.
2) Klicken Sie auf **OK & Weiter**.

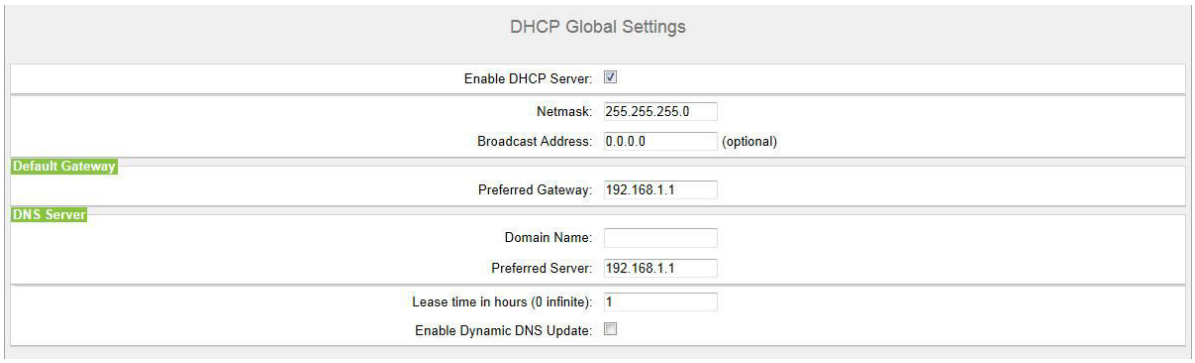
Nächste Schritte

Länder- und Zeiteinstellungen konfigurieren.

4.6.3.2 Wie Sie den internen DHCP-Server aktivieren und konfigurieren

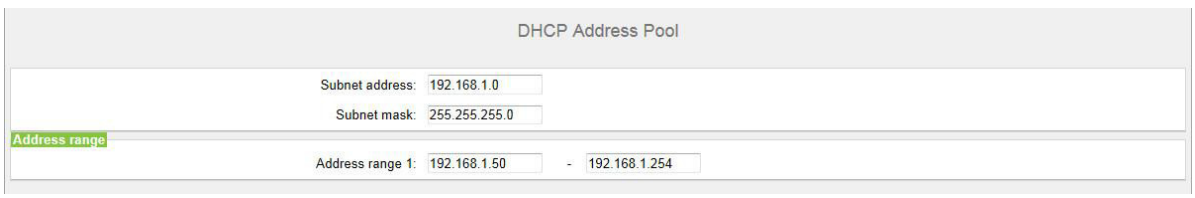
Voraussetzungen

- Im internen Netz ist der externe DHCP-Server (z. B. der DHCP-Server des Internet-Routers) deaktiviert.
- Sie befinden sich im Fenster **DHCP globale Einstellungen**.



Schritt für Schritt

1) Lassen Sie das Kontrollkästchen **DHCP-Server aktivieren** aktiviert.
2) Passen Sie im Feld **Netzmaske** die Netzmaske an Ihren IP-Adressbereich an (z. B. `255.255.255.0`).
3) Geben Sie in dem Feld **Bevorzugtes Gateway** die IP-Adresse des Internet-Routers ein (z. B. `192.168.1.1`).
4) Geben Sie in dem Feld **Bevorzugter Server** die IP-Adresse des DNS-Servers ein (z. B. die IP-Adresse des Internet-Routers, `192.168.1.1`).
5) Klicken Sie auf **OK & Weiter**. Es erscheint das Fenster **DHCP-Address-Pool**.



6) Definieren Sie in den Feldern **Subnetz Adresse**, **Netzmaske** und **Adressbereich 1** den IP-Adressbereich, den der interne DHCP-Server verwalten soll.

Werden im internen Netz feste IP-Adressen verwendet (z. B. für einen Drucker-Server), muss der IP-Adressbereich (DHCP-Adress-Pool) so gewählt werden, dass die festen IP-Adressen nicht innerhalb des IP-Adressbereichs liegen.

Beispiel:

Internet-Router: `192.168.1.1`

OpenScape Business: `192.168.1.2`

UC Booster Card: `192.168.1.3`

Subnetz Adresse: `192.168.1.0`

Netzmaske: `255.255.255.0`

Drucker-Server: `192.168.1.10`

DHCP-Adress-Pool: `192.168.1.50` bis `192.168.1.254`

7) Klicken Sie auf **OK & Weiter**.

Nächste Schritte

Länder- und Zeiteinstellungen konfigurieren.

4.6.4 Länder- und Zeiteinstellungen

Im Fenster **Basiskonfiguration** wählen Sie Ihr Land und die Sprache für die Event-Logs aus und stellen Datum und Uhrzeit ein. Wenn Sie die integrierte Cordless-Lösung nutzen, geben Sie hier die systemweite DECT-Systemkennung ein.

Gehen Sie folgendermaßen vor:

1. Länderkennzeichen und Sprache für Event-Logs auswählen
   Für eine korrekte Länderinitialisierung müssen Sie das Land auswählen, in dem das Kommunikationssystem betrieben wird. Zusätzlich können Sie die Sprache auswählen, in der die Event-Logs (Protokolle für Systemereignisse, Fehler, usw.) abgespeichert werden.
2. DECT-Systemkennung eingeben (nur bei integrierter Cordless-Lösung)
   Wenn Sie die integrierte Cordless-Lösung nutzen, geben Sie hier die systemweite DECT-Systemkennung ein.
3. Datum und Uhrzeit einstellen
   - Datum und Uhrzeit manuell einstellen
     Kommunikationssystem und Teilnehmer (IP-Telefone, TDM-Telefone, Client-PCs) sollten über eine einheitliche Zeitbasis (Datum und Uhrzeit) verfügen. Ist für die Zeitsynchronisation kein SNTP-Server bekannt, können Sie Datum und Uhrzeit auch manuell eingeben.

INFO: Datum und Uhrzeit werden auch aktualisiert, wenn eine Verbindung über eine ISDN-Amtsleitung aufgebaut wird.

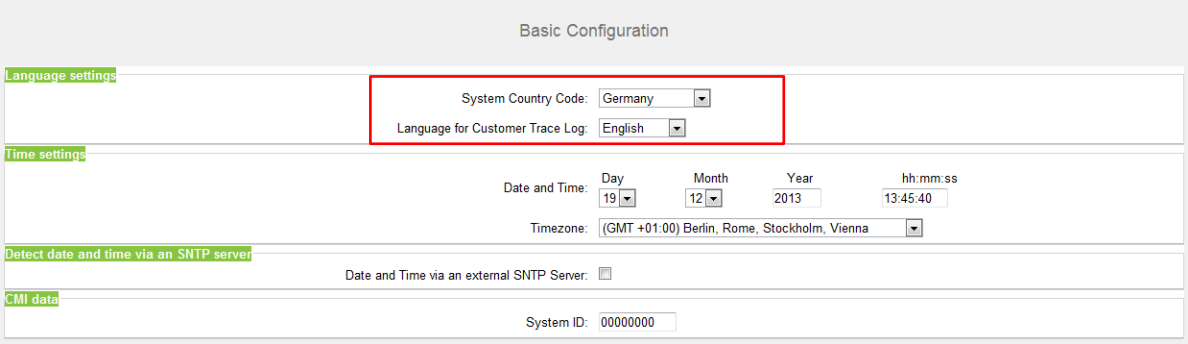
- Datum und Uhrzeit von einem SNTP-Server beziehen
  Kommunikationssystem und IP-Teilnehmer (IP-Telefone, Client-PCs) sollten über eine einheitliche Zeitbasis (Datum und Uhrzeit) verfügen. Diese Zeitbasis kann von einem SNTP-Server zur Verfügung gestellt werden. Der SNTP-Server kann sich im internen Netz oder im Internet befinden.

Die IP-Telefone erhalten Datum & Uhrzeit automatisch vom Kommunikationssystem. Die Client-PCs, auf denen die UC-Clients laufen, müssen so eingestellt sein, dass sie zeitsynchron mit dem Kommunikationssystem sind (siehe Anleitung des Betriebssystems der Client-PCs).

4.6.4.1 Wie Sie das Länderkennzeichen und die Sprache für Event-Logs auswählen

Voraussetzungen

- Sie befinden sich im Fenster **Basiskonfiguration**.



Schritt für Schritt

1) Wählen Sie in der Aufklappliste **System-Länderkennzeichen** das Land aus, in dem das Kommunikationssystem betrieben wird.

2) Wählen Sie im Feld **Sprache für Kunden-Eventlog** die Sprache aus, in der die Event-Logs (Protokolle für Systemereignisse, Fehler, usw.) ausgegeben werden sollen.

Nächste Schritte

DECT-Systemkennung eingeben (nur bei integrierter Cordless-Lösung)

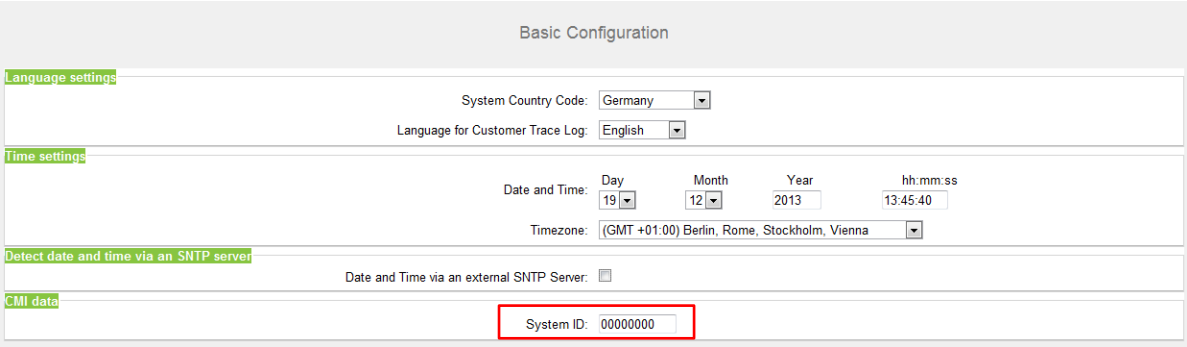
oder

Datum und Uhrzeit manuell einstellen oder Datum und Uhrzeit von einem SNTP-Server beziehen.

4.6.4.2 Wie Sie die DECT-Systemkennung eingeben

Voraussetzungen

- Sie befinden sich im Fenster **Basiskonfiguration**.



Schritt für Schritt

› Geben Sie im Bereich **CMI Daten** unter **Systemkennung** die 8-stellige, hexadezimale DECT-Systemkennung ein, die Sie beim Erwerb Ihrer integrierten Cordless-Lösung erhalten haben.

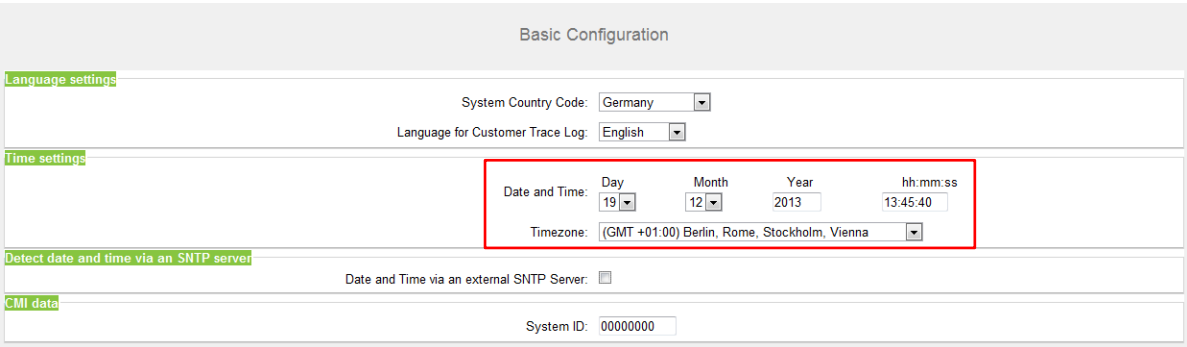
Nächste Schritte

Datum und Uhrzeit manuell einstellen oder Datum und Uhrzeit von einem SNTP-Server beziehen.

4.6.4.3 Wie Sie Datum und Uhrzeit manuell einstellen

Voraussetzungen

- Sie befinden sich im Fenster **Basiskonfiguration**.



Schritt für Schritt

1) Geben Sie die aktuellen Werte für **Datum und Uhrzeit** ein.

2) Wählen Sie im Feld **Zeitzone** die gewünschte Zeitzone aus.

3) Klicken Sie auf **OK & Weiter**.

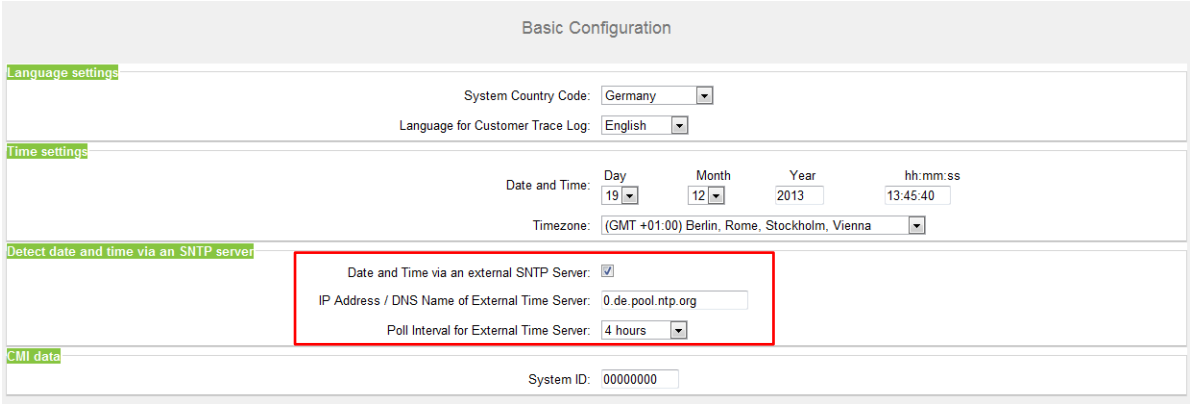
Nächste Schritte

UC-Lösung festlegen.

4.6.4.4 Wie Sie Datum und Uhrzeit von einem SNTP-Server beziehen

Voraussetzungen

- Sie befinden sich im Fenster **Basiskonfiguration**.



Schritt für Schritt

1) Aktivieren Sie das Kontrollkästchen **Datum und Uhrzeit über externen SNTP Server**.
2) Geben Sie im Feld **IP-Adresse / DNS-Name des externen Zeitservers** die IP-Adresse oder den DNS-Namen des SNTP-Servers ein (z. B. `0.de.pool.ntp.org`).
3) Wählen Sie aus der Aufklappliste **Pollzeit für externen Zeitserver** aus, nach wie vielen Stunden Datum und Uhrzeit vom SNTP-Server synchronisiert werden sollen (empfohlen `4 h`).
4) Klicken Sie auf **OK & Weiter**.

Nächste Schritte

UC-Lösung festlegen.

4.6.5 UC-Lösung

Im Fenster **Applikationsauswahl ändern** legen Sie fest, welche UC-Lösung Sie nutzen.

Sie haben folgende Möglichkeiten:

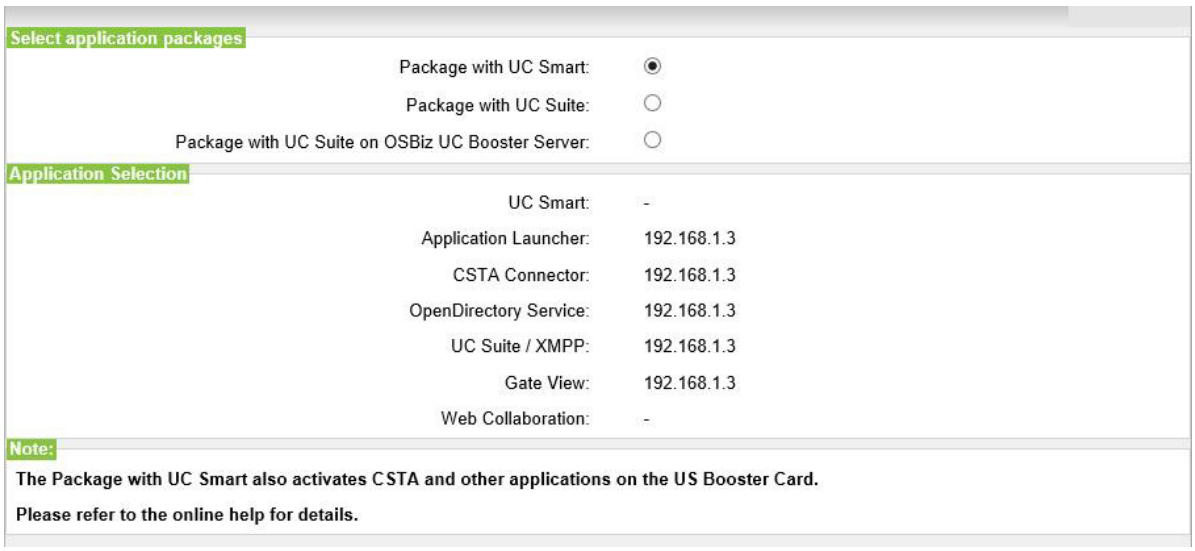
- **Paket mit UC Smart**
  Die UC-Lösung UC Smart ist auf dem Mainboard intergiert.

- **Paket mit UC Suite**
  Die UC-Lösung UC Suite ist auf der internen Baugruppe "UC Booster Card" intergiert.
- **Paket mit UC Suite auf OSBiz UC Booster-Server**
  Die UC-Lösung UC Suite ist auf dem externen Linux-Server "OpenScape Business UC Booster Server" intergiert.

4.6.5.1 Wie Sie die UC-Lösung festlegen

Voraussetzungen

- Sie haben Lizenzen erworben entweder für die UC-Lösung UC Smart oder für die UC-Lösung UC Suite.
- Sie befinden Sich im Fenster **Applikationsauswahl ändern**.



Schritt für Schritt

1) Wenn Sie die UC-Lösung UC Smart nutzen, klicken Sie auf **Paket mit UC Smart**.

2) Wenn Sie die UC-Lösung UC Suite nutzen, die auf der internen Baugruppe "UC Booster Card" integriert ist, klicken Sie auf **Paket mit UC Suite**.

3) Wenn Sie die UC-Lösung UC Suite nutzen, die auf dem externen Linux-Server "OpenScape Business UC Booster Server" integriert ist, klicken Sie auf **Paket mit UC Suite auf OSBiz UC Booster-Server**. Geben Sie zusätzlich im Feld **IP-Adresse des OSBiz UC Booster-Servers** die IP-Adresse des externen Linux-Servers an.

4) Klicken Sie auf **OK & Weiter**.

5) Der Wizard **Erstinstallation** ist abgeschlossen. Klicken Sie auf **Beenden**.

6) Beenden Sie das WBM, indem Sie rechts oben auf den Link **Abmelden** klicken und anschließend das Fenster schließen.

INFO: Wurden IP-Adressen oder Einstellungen des DHCP-Servers geändert, führt das Kommunikationssystem einen Neustart durch. Dies kann einige Minuten dauern.

Nächste Schritte

Kommunikationssystem ans Kunden-LAN anschließen.

4.6.6 Anschluss des Kommunikationssystems ans Kunden-LAN

Nach erfolgreicher Erstinstallation wird das Kommunikationssystem an das bestehende Kunden-LAN angeschlossen.

4.6.6.1 Wie Sie das Kommunikationssystem ans Kunden-LAN anschließen

Voraussetzungen

- Das Kommunikationssystem ist betriebsbereit.

Schritt für Schritt

1) Entfernen Sie das LAN-Kabel des Admin-PC aus der mittleren LAN-Schnittstelle "LAN" und integrieren Sie den Admin-PC in das Kunden-LAN, indem Sie ihn z. B. an einen Switch anschließen.

2) Schließen Sie ein LAN-Kabel an die mittlere LAN-Schnittstelle "LAN" des Kommunikationssystems an.

3) Integrieren Sie das Kommunikationssystem über dieses LAN-Kabel in das Kunden-LAN, indem Sie es z. B. an einen Switch anschließen.

4) Ist eine UC Booster Card (Application Board) gesteckt, schließen Sie ein weiteres LAN-Kabel an die LAN-Schnittstelle "LAN2" der UC Booster Card an (rechte/untere der beiden LAN-Schnittstellen) und integrieren Sie die UC Booster Card über dieses LAN-Kabel in das Kunden-LAN, indem Sie es z. B. an einen Switch anschließen.

Nächste Schritte

Basiskonfiguration starten.

4.7 Basiskonfiguration

Die Basiskonfiguration wird mit dem Wizard **Basisinstallation** des WBM durchgeführt. Dabei werden die wichtigsten Einstellungen für den Betrieb des Kommunikationssystems festgelegt.

4.7.1 Wie Sie den Wizard Basisinstallation starten

Voraussetzungen

- Der Wizard **Erstinstallation** ist durchlaufen.
- Das Kommunikationssystem ist ins Kunden-LAN integriert.
- Das Kommunikationssystem ist betriebsbereit. Die LED "Run" des Mainboards blinkt grün im 1Hz-Takt (0,5s an / 0,5s aus).

Schritt für Schritt

1) Rufen Sie auf dem Admin-PC in Ihrem Webbrowser die Anmeldeseite des WBM unter folgender Adresse auf:

`https://<IP-Adresse von OpenScape Business>`

Die Standard-IP-Adresse von OpenScape Business ist `192.168.1.2`, also z. B. `https://192.168.1.2`

2) Geben Sie im Feld **Benutzername** den Standard-Benutzernamen `administrator@system` für den Zugang als Administrator ein.

3) Geben Sie im Feld **Passwort** das von Ihnen während der Erstinbetriebnahme definierte Passwort ein.

4) Klicken Sie auf **Login**.

5) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

6) Klicken Sie auf **Bearbeiten**, um den Wizard **Basisinstallation** zu starten.

Nächste Schritte

Führen Sie die Basisinstallation wie nachstehend beschrieben Schritt für Schritt durch. Felder, die hier nicht beschrieben werden, sind passend für den Standardfall vorbelegt und müssen nur geändert werden, wenn sie nicht zu Ihren Netzwerkdaten passen. Die ausführlichen Informationen finden Sie in der Administratordokumentation bei der Beschreibung der einzelnen Wizards.

4.7.2 Systemrufnummern und Vernetzung

Im Fenster **Übersicht** geben Sie die Systemrufnummern ein (Anlagenrufnummer, Länder- und Ortsvorwahl, Internationales Präfix) und legen fest, ob OpenScape Business mit anderen OpenScape Business Systemen vernetzt werden soll.

Gehen Sie folgendermaßen vor:

1. Systemrufnummern eingeben

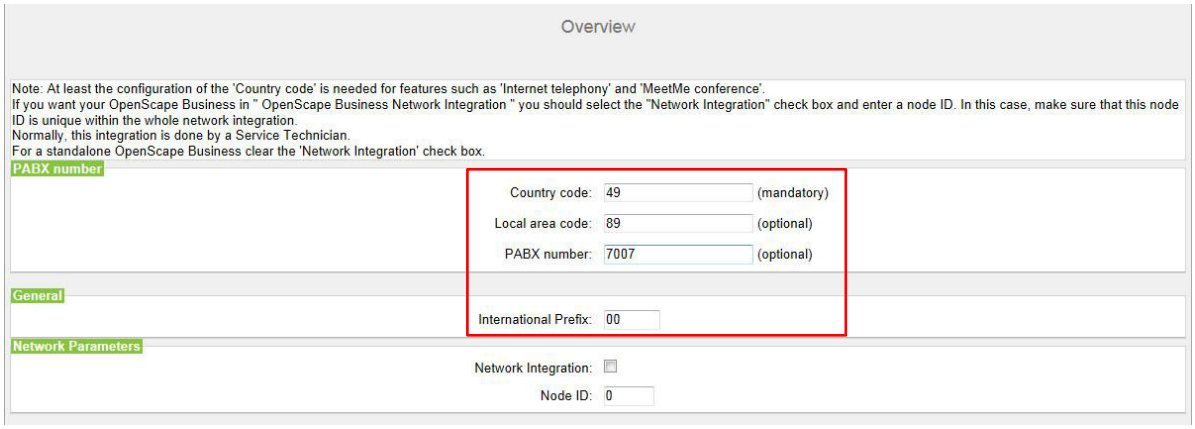
- Systemrufnummern für Anlagenanschluss eingeben
  Hier geben Sie die Anlagenrufnummer für Ihren Anlagenanschluss ein sowie die Länder- und Ortsvorwahl.
  Die Eingabe der Ländervorwahl ist für Internet-Telefonie und Konferenz-Server-Funktionalitäten zwingend erforderlich.
  Das internationale Präfix ist abhängig von der zuvor gewählten Länderkennzahl vorbelegt.
- Systemrufnummern für Mehrgeräteanschluss eingeben
  Hier geben Sie Länder- und Ortsvorwahl für Ihren Mehrgeräteanschluss ein.
  Die Eingabe der Ländervorwahl ist für Internet-Telefonie und für MeetMee-Konferenzen zwingend erforderlich.
  Das internationale Präfix ist abhängig von der zuvor gewählten Länderkennzahl vorbelegt.

2. Vernetzung aktivieren oder deaktivieren
   Soll OpenScape Business mit anderen OpenScape Business Systemen vernetzt werden, muss die Vernetzung aktiviert und OpenScape Business eine Knoten-ID zugewiesen werden. Jede OpenScape Business muss im Netzverbund eine eindeutige Knoten-ID besitzen.

4.7.2.1 Wie Sie die Systemrufnummern für einen Anlagenanschluss eingeben

Voraussetzungen

- Sie haben einen Anlagenanschluss.
- Sie befinden sich im Fenster **Übersicht**.



Schritt für Schritt

1) Geben Sie im Feld **Ländervorwahl** die Ländervorwahl ein, z. B. `49` für Deutschland oder `1` für USA.

2) Geben Sie im Feld **Ortsnetzkennzahl** die Ortsvorwahl ein, z. B. `89` für München.

3) Geben Sie im Feld **Anlagenrufnummer** die Anlagenrufnummer Ihres Amtsanschlusses ein, z. B. `7007` (Ihre Anschlussnummer).

4) Ändern Sie das Feld **Internationales Präfix** nur wenn nötig. Für Deutschland gilt `00`, für USA `011`).

Bei Telefonaten ins Ausland wird der Telefonnummer das internationale Präfix und die Ländervorwahl vorangestellt, z. B. bei einem Telefonat von Deutschland nach USA die "00-1-..." und bei einem Telefonat von USA nach Deutschland die "011-49-...".

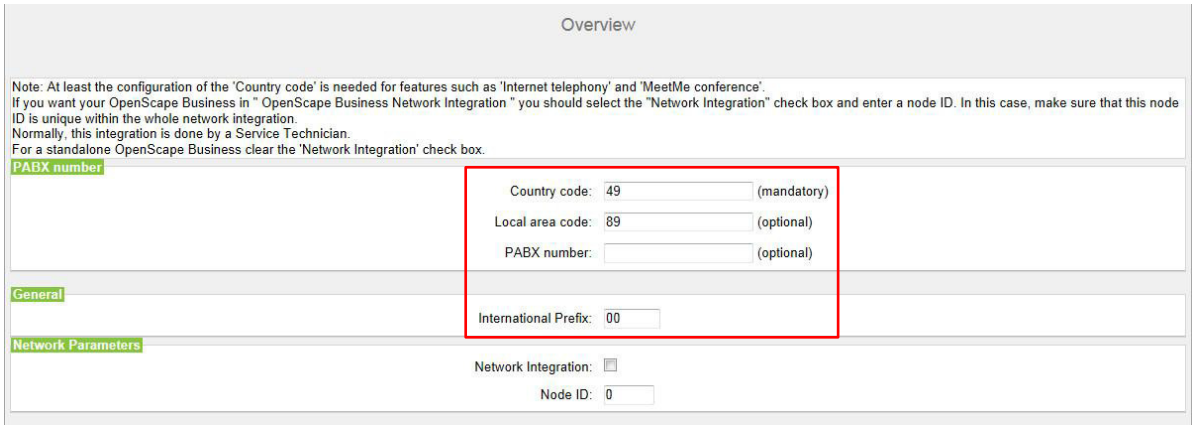
Nächste Schritte

Vernetzung aktivieren oder deaktivieren.

4.7.2.2 Wie Sie die Systemrufnummern für einen Mehrgeräteanschluss eingeben

Voraussetzungen

- Sie haben einen Mehrgeräteanschluss.
- Sie befinden sich im Fenster **Übersicht**.



Schritt für Schritt

1) Geben Sie im Feld **Ländervorwahl** die Ländervorwahl ein, z. B. `49` für Deutschland oder `1` für USA.

2) Geben Sie im Feld **Ortsnetzkennzahl** die Ortsvorwahl ein, z. B. `89` für München.

3) Lassen Sie das Feld **Anlagenrufnummer** leer.

4) Ändern Sie das Feld **Internationales Präfix** nur wenn nötig. Für Deutschland gilt `00`, für USA `011`).

Bei Telefonaten ins Ausland wird der Telefonnummer das internationale Präfix und die Ländervorwahl vorangestellt, z. B. bei einem Telefonat von Deutschland nach USA die "00-1-..." und bei einem Telefonat von USA nach Deutschland die "011-49-...".

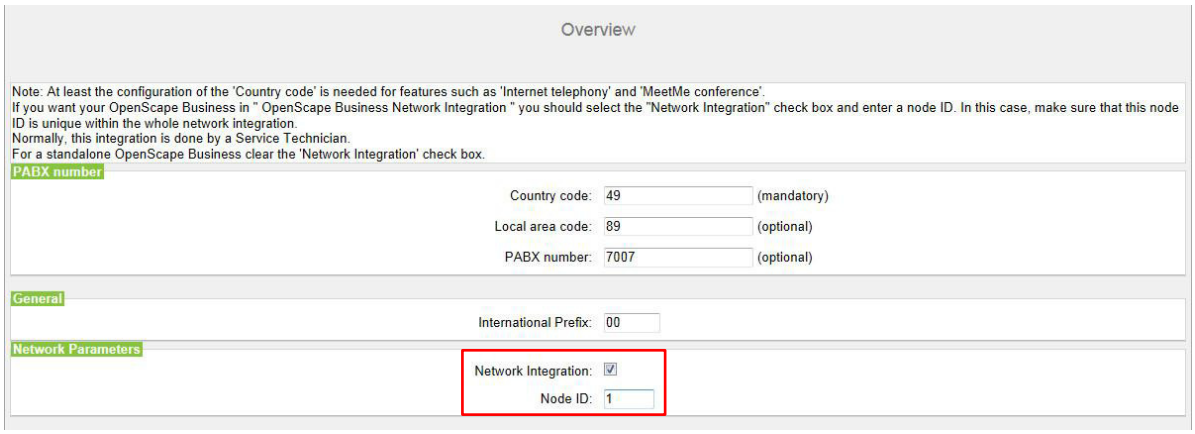
Nächste Schritte

Vernetzung aktivieren oder deaktivieren.

4.7.2.3 Wie Sie die Vernetzung aktivieren oder deaktivieren

Voraussetzungen

- Sie befinden sich im Fenster **Übersicht**.



Schritt für Schritt

1) Wenn das Kommunikationssystem mit anderen Kommunikationssystemen vernetzt werden soll:

a) Aktivieren Sie das Kontrollkästchen **Netzwerk-Integration**.

b) Vergeben Sie im Feld **Knoten-ID** für das Kommunikationssystem eine im Netzverbund eindeutige Knoten-ID (Ziffern von `1` bis `100` möglich).

2) Wenn das Kommunikationssystem nicht mit anderen Kommunikationssystemen vernetzt werden soll, lassen Sie das Kontrollkästchen **Netzwerk-Integration** deaktiviert.

3) Klicken Sie auf **OK & Weiter**.

Nächste Schritte

Teilnehmerdaten konfigurieren.

4.7.3 Teilnehmerdaten

Im Fenster **Zentrale Teilnehmer-Funktionen** können Sie bei Bedarf anstelle des vordefinierten Standardrufnummernplans Ihren individuellen Rufnummernplan konfigurieren und weitere Teilnehmerdaten importieren. Im Netzverbund muss der Standard-Rufnummernplan an den Rufnummernplan des Netzverbunds angepasst werden.

Der Standardrufnummernplan enthält vordefinierte Rufnummern für verschiedene Teilnehmertypen (IP-Telefone, analoge Telefone, ...) und für spezielle Funktionen (Internet-Telefonie, Sprachbox, AutoAttendant, ...).

Die Teilnehmerdaten enthalten u.a. die internen Rufnummern, die Durchwahlnummern und die Namen der Teilnehmer. Über eine XML-Datei im UTF-8-Format können diese Daten und weitere Teilnehmerdaten während der Basiskonfiguration in das Kommunikationssystem importiert werden.

INFO: Eine XML-Vorlage mit zugehöriger Erklärung finden Sie im WBM unter **Service-Center > Dokumente > CSV-Vorlagen**. In diese Vorlage können Sie z. B. mit Microsoft Excel Ihre Daten eintragen.

Sie haben folgende Möglichkeiten:

- **Teilnehmerdaten ohne Netzverbund konfigurieren**
  Gehen Sie folgendermaßen vor:

  a) Teilnehmerdaten anzeigen
  Sie können sich alle vorkonfigurierten Rufnummern und Teilnehmerdaten anzeigen lassen.

  b) Alle Rufnummern löschen (optional)
  Verwenden Sie einen individuellen Rufnummernplan, müssen Sie alle vorkonfigurierten Rufnummern löschen.

  c) Vorkonfigurierte Rufnummern an den individuellen Rufnummernplan anpassen (optional)
  Verwenden Sie einen individuellen Rufnummernplan, können Sie die vorkonfigurierten Rufnummern an den eigenen Rufnummernplan anpassen.

  d) Teilnehmerdaten über XML-Datei importieren (optional)
  Ihre individuellen Rufnummern inkl. zusätzlicher Teilnehmerdaten können Sie bequem über eine XML-Datei während der Basiskonfiguration importieren.

- **Teilnehmerdaten mit Netzverbund konfigurieren**
  Gehen Sie folgendermaßen vor:

  a) Alle Rufnummern löschen
  Falls im Netzverbund die UC Suite zum Einsatz kommt, ist ein geschlossener Rufnummernplan erforderlich, d.h. alle Rufnummern im Netzverbund müssen eindeutig sein. Daher müssen die vorkonfigurierten Rufnummern gelöscht und an den Netzverbund angepasste Rufnummern verwendet werden.

  b) Teilnehmerdaten über XML-Datei importieren
  Die an den Netzverbund angepassten Rufnummern sind inkl. zusätzlicher Teilnehmerdaten bequem über eine XML-Datei während der Basiskonfiguration zu importieren. Diese Datei kann alle Teilnehmer des Netzverbundes enthalten. Beim Import werden nur die Rufnummern und Teilnehmerdaten übernommen, die der zuvor angegebenen Knoten-ID des Kommunikationssystems zugeordnet sind.

4.7.3.1 Wie Sie die Teilnehmerdaten anzeigen

Voraussetzungen

- Sie befinden sich im Fenster **Zentrale Teilnehmer-Funktionen**.

Schritt für Schritt

1) Aktivieren Sie das Optionsfeld **Teilnehmerkonfiguration anzeigen**.

2) Klicken Sie auf **Funktion ausführen**. Es wird Ihnen eine Liste der Teilnehmer mit den vorkonfigurierten Rufnummern (Standard-Rufnummernplan) angezeigt.

3) Klicken Sie auf **OK**. Sie werden zum Fenster **Zentrale Teilnehmer-Funktionen** zurückgeführt.

4) Wenn Sie keine Teilnehmerdaten ändern wollen, klicken Sie auf **OK & Weiter**.

4.7.3.2 Wie Sie alle Rufnummern löschen

Voraussetzungen

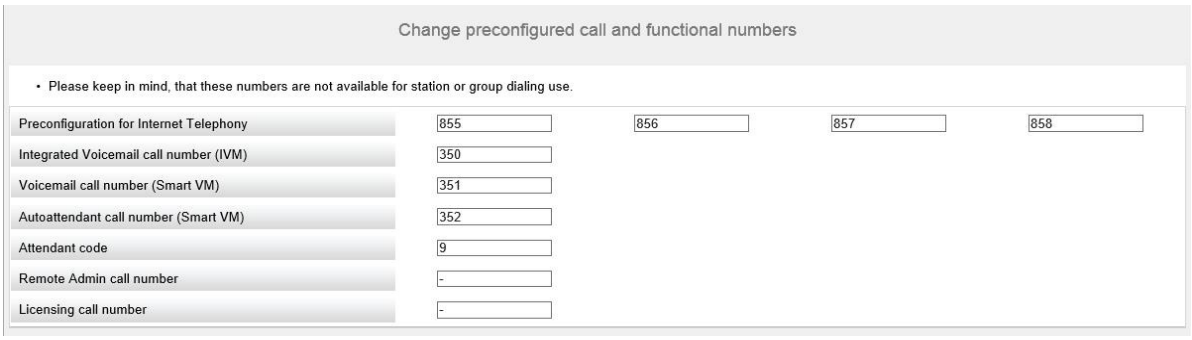
- Sie befinden sich im Fenster **Zentrale Teilnehmer-Funktionen**.

Schritt für Schritt

1) Aktivieren Sie das Optionsfeld **Alle Rufnummern löschen**.

2) Aktivieren Sie das Kontrollkästchen **Alle Rufnummern löschen**.

3) Klicken Sie auf **Funktion ausführen**. Alle vorbelegten Rufnummern werden gelöscht. Anschließend erscheint das Fenster **Vorkonfigurierte Rufnummern ändern**.



4) Passen Sie die Kennzahlen und speziellen Rufnummern an Ihre Wünsche an und klicken Sie anschließend auf **OK**. Sie werden zum Fenster **Zentrale Teilnehmer-Funktionen** zurückgeführt.

5) Wenn Sie keine weiteren Teilnehmerdaten ändern wollen, klicken Sie auf **OK & Weiter**.

4.7.3.3 Vorkonfigurierte Rufnummern an den individuellen Rufnummernplan anpassen

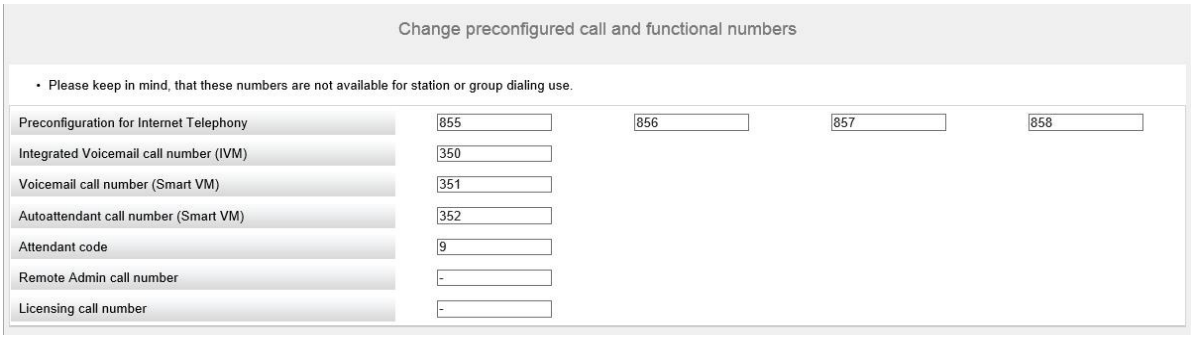
Voraussetzungen

- Sie befinden sich im Fenster **Zentrale Teilnehmer-Funktionen**.

Schritt für Schritt

1) Aktivieren Sie das Optionsfeld **Vorkonfigurierte Rufnummern ändern**.

2) Klicken Sie auf **Funktion ausführen**. Es erscheint das Fenster **Vorkonfigurierte Rufnummern ändern**.



3) Passen Sie die vorkonfigurierten Rufnummern an Ihre Wünsche an und klicken Sie anschließend auf **OK**. Sie werden zum Fenster **Zentrale Teilnehmer-Funktionen** zurückgeführt.

4) Wenn Sie keine weiteren Teilnehmerdaten ändern wollen, klicken Sie auf **OK & Weiter**.

4.7.3.4 Wie Sie die Teilnehmerdaten über eine XML-Datei importieren

Voraussetzungen

- Sie befinden sich im Fenster **Zentrale Teilnehmer-Funktionen**.
- Eine XML-Datei im UTF-8-Format mit den eingetragenen Daten liegt vor. Eine XML-Vorlage finden Sie unter **Service-Center > Dokumente > CSV-Vorlagen**.

Schritt für Schritt

1) Aktivieren Sie das Optionsfeld **XML-Datei mit Teilnehmerdaten importieren**.

2) Klicken Sie auf **Funktion ausführen**.

3) Wählen Sie mit **Durchsuchen** die erstellte XML-Datei aus und klicken Sie auf **Öffnen**.

4) Klicken Sie anschließend auf **OK**. Die Teilnehmerdaten werden importiert.

5) Klicken Sie auf **OK & Weiter**.

4.7.4 ISDN-Konfiguration

Im Fenster **ISDN-Konfiguration** legen Sie fest, ob ISDN-Teilnehmer angeschlossen werden sollen und ob der Amtsanschluss über ISDN erfolgen soll. Der ISDN-Amtsanschluss kann als ISDN-Anlagenanschluss und/oder ISDN-Mehrgeräteanschluss eingerichtet werden. Je nach Kommunikationssystem und evtl. verwendeter Baugruppe stehen dafür unterschiedlich viele S_0-Schnittstellen zur Verfügung.

Sie haben folgende Möglichkeiten:

- ISDN-Konfiguration aktivieren:
  a) ISDN-Anlagenanschluss konfigurieren
  Sie können einen ISDN-Amtsanschluss als Anlagenanschluss mit Durchwahlnummern einrichten.
  b) ISDN-Mehrgeräteanschluss konfigurieren
  Sie können einen ISDN-Amtsanschluss als Mehrgeräteanschluss mit MSN einrichten.
  c) Anschluss von ISDN-Teilnehmern konfigurieren (optional)
  Eine oder mehrere S_0-Schnittstellen können als interne S_0-Anschlüsse konfiguriert werden, um ISDN-Teilnehmer (ISDN-Telefon oder ISDN-Fax) daran anzuschließen. Für jeden ISDN-Teilnehmer benötigen Sie eine Teilnehmer-Lizenz.
- ISDN-Konfiguration deaktivieren
  Wenn Sie keinen ISDN-Amtsanschluss haben, müssen Sie die ISDN-Konfiguration deaktivieren. Alle S_0-Schnittstellen werden automatisch als interne S_0-Anschlüsse konfiguriert.

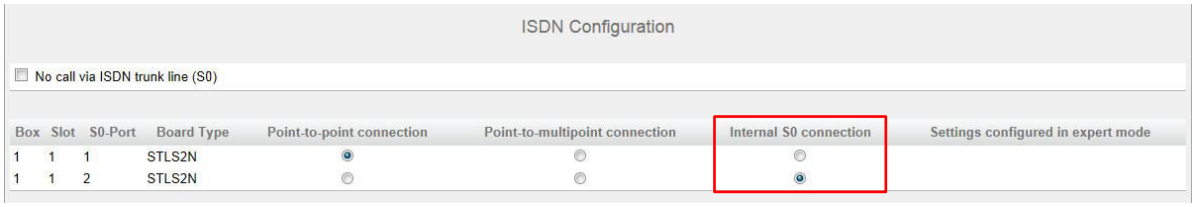
Weitere Möglichkeiten für einen Amtsanschluss

Anstelle des ISDN-Amtsanschlusses können Sie auch einen analogen Amtsanschluss oder einen Amtsanschluss über einen Internet-Telefonie-Service-Provider (ITSP, SIP-Provider) einrichten. Die Konfiguration des analogen Amtsanschlusses ist erst nach Abschluss der Basisinstallation möglich.

4.7.4.1 Wie Sie den Anschluss von ISDN-Teilnehmern konfigurieren

Voraussetzungen

- Sie befinden sich im Fenster **ISDN-Konfiguration**.



Schritt für Schritt

1) Lassen Sie das Kontrollkästchen **Keine Telefonie über ISDN-Amtsleitung (S0)** deaktiviert.
2) Aktivieren Sie bei der gewünschten S_0-Schnittstelle das Optionsfeld **interner S0-Anschluss**.

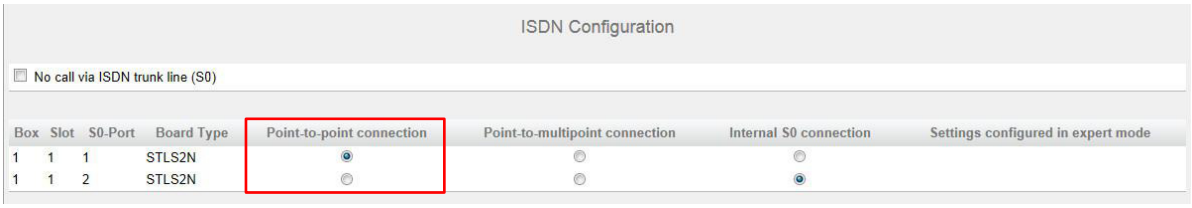
Nächste Schritte

ISDN-Anlagenanschluss konfigurieren und/oder ISDN-Mehrgeräteanschluss konfigurieren.

4.7.4.2 Wie Sie den ISDN-Anlagenanschluss konfigurieren

Voraussetzungen

- Sie befinden sich im Fenster **ISDN-Konfiguration**.



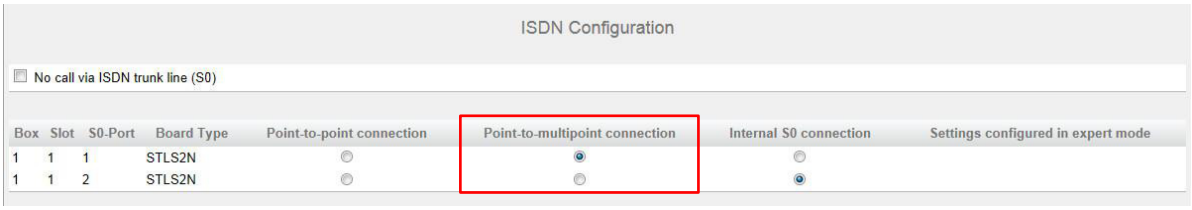
Schritt für Schritt

1) Um den ISDN-Amtsanschluss einzurichten, lassen Sie das Kontrollkästchen **Keine Telefonie über ISDN-Amtsleitung (S0)** deaktiviert.
2) Aktivieren Sie bei dem gewünschten S_0-Anschluss das Optionsfeld **Anlagenanschluss**.
3) Klicken Sie auf **OK & Weiter**.

4.7.4.3 Wie Sie den ISDN-Mehrgeräteanschluss konfigurieren

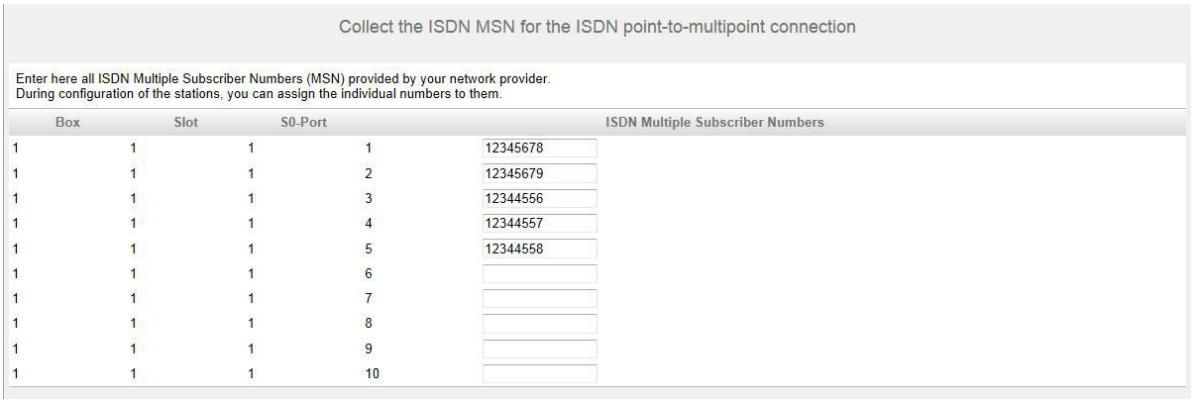
Voraussetzungen

- Sie befinden sich im Fenster **ISDN-Konfiguration**.



Schritt für Schritt

1) Um den ISDN-Amtsanschluss einzurichten, lassen Sie das Kontrollkästchen **Keine Telefonie über ISDN-Amtsleitung (S0)** deaktiviert.
2) Aktivieren Sie bei dem gewünschten S_0-Anschluss das Optionsfeld **Mehrgeräteanschluss**.
3) Klicken Sie auf **OK & Weiter**.



4) Geben Sie in der Spalte **ISDN-Mehrfachrufnummern** alle Rufnummern (MSN) ein, die Ihnen Ihr Netzanbieter mitgeteilt hat. Pro S_0-Anschluss können Sie bis zu 10 MSN eingeben. Die Anzahl der S_0-Anschlüsse ist abhängig vom Kommunikationssystem und von der evtl. verwendeten Baugruppe.
5) Klicken Sie auf **OK & Weiter**.

4.7.4.4 Wie Sie die ISDN-Konfiguration deaktivieren

Voraussetzungen

- Sie befinden sich im Fenster **ISDN-Konfiguration**.

Schritt für Schritt

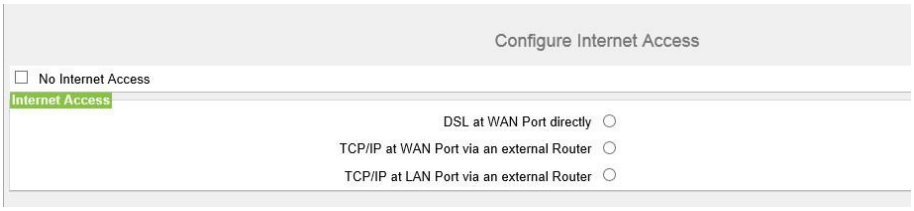
1) Aktivieren Sie das Kontrollkästchen **Keine Telefonie über ISDN-Amtsleitung (S0)**.

> ***INFO:*** Gespräche können auch über einen Internet-Telefonie-Service-Provider geführt werden, siehe *Internet-Telefonie*.

2) Klicken Sie auf **OK & Weiter**.

4.7.5 Internet-Zugang

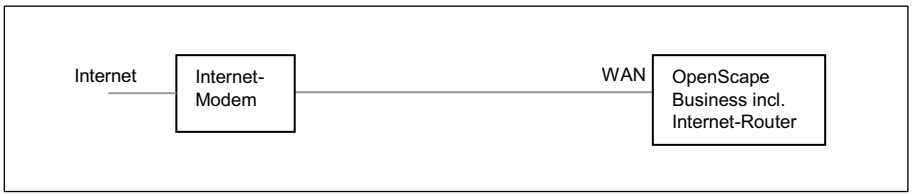
Im Fenster **Konfiguration des Internetzugangs** konfigurieren Sie den Internet-Zugang.



Die Konfiguration des Internet-Zugangs im WBM ist davon abhängig, ob der Internet-Zugang bereits in einem externen Router eingerichtet ist oder ob er über ein Internet-Modem erfolgt und somit im WBM eingerichtet werden muss.

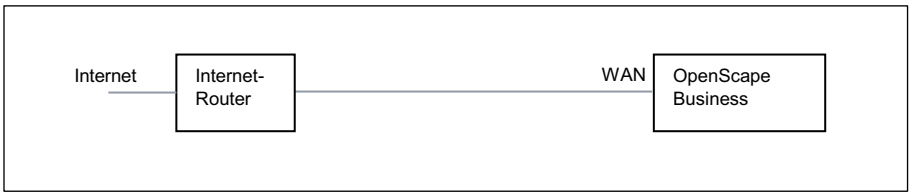
Von den hier aufgeführten Möglichkeiten ist nur eine auszuwählen.

- Internet-Zugang über ein Internet-Modem (**DSL am WAN Port direkt**)
  Sie wollen das Kommunikationssystem direkt an einem Internet-Modem (DSL, Kabel, UMTS ...) betreiben. OpenScape Business hat den Internet-Router integriert. Geben Sie die Zugangsdaten des Internet-Service-Providers (ISP) direkt im Kommunikationssystem ein und nutzen den WAN-Anschluss des Kommunikationssystems.



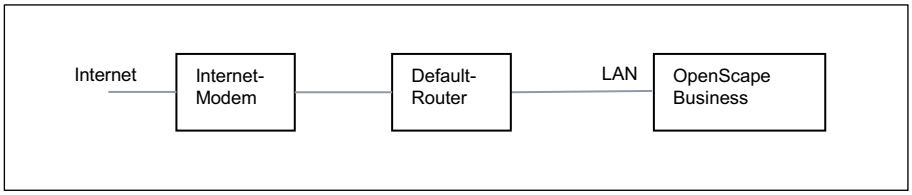
  Sie haben folgende Möglichkeiten:
  - **Internet-Zugang über vorkonfigurierten ISP**
  - **Internet-Zugang über Standard-ISP PPPoE**
  - **Internet-Zugang über Standard-ISP PPTP**

  Ist Ihr ISP nicht unter den vorkonfigurierten ISP, verwenden Sie den Standard-ISP PPPoE oder PPTP.
- Internet-Zugang über einen externen Internet-Router
  Sie wollen das Kommunikationssystem an einem externen Internet-Router betreiben. Der Internet-Service-Provider ist bereits im Internet-Router konfiguriert.
  Sie haben folgende Möglichkeiten:
  - **Internet-Zugang über externen Internet-Router am WAN-Anschluss** (**TCP/IP am WAN Port über einen externen Router**)



    Dazu nutzen Sie den WAN-Anschluss des Kommunikationssystems. OpenScape Business kennt entweder den Internet-Router oder arbeitet als DHCP-Client. Diese Möglichkeit kann verwendet werden, wenn der Internet-Router in einem anderen Netzsegment liegt und einen eigenen DHCP-Server hat.

– **Internet-Zugang über externen Internet-Router am LAN-Anschluss** (**TCP/IP am LAN Port über einen externen Router**)



Dazu nutzen Sie den LAN-Anschluss des Kommunikationssystems. OpenScape Business kennt nur den Default-Router und nicht die dahinterliegende Infrastruktur. Um die Verbindung zum Internet-Router zu aktivieren, muss dem Kommunikationssystem die IP-Adresse des Default-Routers und des DNS-Servers bekannt gegeben werden.

- Internet-Zugang deaktivieren (Standardeinstellung)
  Sie wollen das Internet nicht nutzen.

4.7.5.1 Wie Sie den Internet-Zugang über einen externen Internet-Router über den LAN-Anschluss konfigurieren

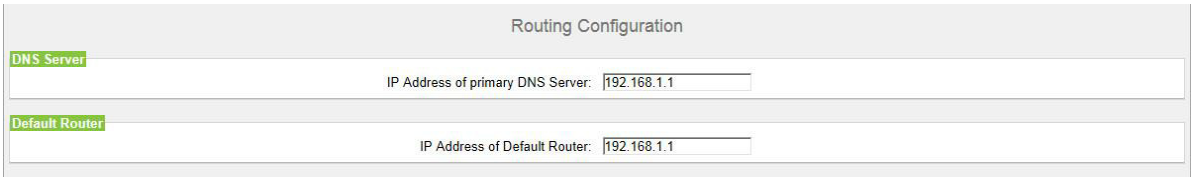
Voraussetzungen

- Das Kommunikationssystem muss über die LAN-Schnittstelle "LAN" mit dem Kunden-LAN verbunden sein. Die Verbindung darf nicht über den WAN-Anschluss erfolgen, da dieser deaktiviert wird.
- Sie befinden sich im Fenster **Konfiguration des Internetzugangs**.

Schritt für Schritt

1) Deaktivieren Sie das Kontrollkästchen **Kein Internet-Zugang**.

2) Aktivieren Sie das Optionsfeld **TCP/IP am LAN Port über einen externen Router** und klicken Sie auf **OK & Weiter**.



3) Geben Sie im Feld **IP-Adresse des bevorzugten DNS-Servers** die IP-Adresse des lokalen DNS-Servers (z. B. Internet-Router) oder des Internet-DNS-Servers (z. B. für Internet-Telefonie) ein.

4) Geben Sie im Feld **IP-Adresse des Default Routers** die IP-Adresse des externen Internet-Routers ein.

5) Klicken Sie auf **OK & Weiter**.

4.7.5.2 Wie Sie den Internet-Zugang über einen externen Internet-Router über den WAN-Anschluss konfigurieren

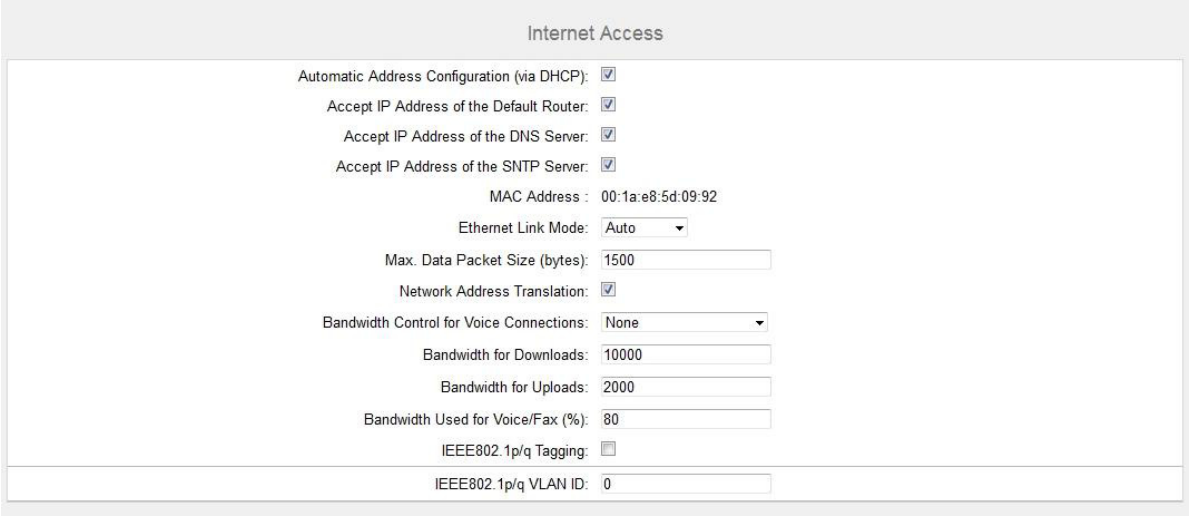
Voraussetzungen

- Das Kommunikationssystem muss über die LAN-Schnittstelle "WAN" mit dem LAN-Segment des Kunden-LAN verbunden sein, indem sich der Internet-Router befindet.
- Sie befinden sich im Fenster **Konfiguration des Internetzugangs**.

Schritt für Schritt

1) Deaktivieren Sie das Kontrollkästchen **Kein Internet-Zugang**.

2) Aktivieren Sie das Optionsfeld **TCP/IP am WAN Port über einen externen Router** und klicken Sie auf **OK & Weiter**.



3) Wenn für die WAN-Schnittstelle die netzwerkspezifischen Daten von einem bereits aktiven DHCP-Server bezogen werden sollen:

a) Aktivieren Sie das Kontrollkästchen **Automatische Adresskonfiguration (mit DHCP)**.

b) Aktivieren Sie das Kontrollkästchen **IP-Adresse des Default Routers übernehmen**.

c) Aktivieren Sie bei Bedarf das Kontrollkästchen **IP-Adresse des DNS-Servers übernehmen**.

d) Aktivieren Sie bei Bedarf das Kontrollkästchen **IP-Adresse des SNTP-Servers übernehmen**.

4) Wenn der WAN-Schnittstelle eine feste IP-Adresse zugeordnet werden soll:

a) Deaktivieren Sie das Kontrollkästchen **Automatische Adresskonfiguration (mit DHCP)**.

b) Geben Sie die gewünschte **IP-Adresse** und **Netzmaske** der WAN-Schnittstelle ein.

5) Aktivieren Sie das Kontrollkästchen **Netzwerkaddressübersetzung (NAT)**.

6) Wenn Sie zusätzlich Internet-Telefonie nutzen wollen, wählen Sie aus der Aufklappliste **Bandbreitensteuerung für Sprach-Verbindungen** den Eintrag **Nur Upload** oder **Upload und Download** je nach Bedarf aus. Bei einer hohen Download-Bandbreite und zugleich niedrigen Upload-Bandbreite sollte die Bandbreitensteuerung nur für den Upload aktiviert werden, damit nicht unnötig viel Download-Bandbreite für die Sprachübertragung reserviert wird.

7) Geben Sie in den Feldern **Bandbreite Download** und **Bandbreite Upload** die Bandbreite in kbit/s für den Download und Upload ein, die Ihnen Ihr Internet-Service-Provider zur Verfügung stellt.

8) Klicken Sie auf **OK & Weiter**.

4.7.5.3 Wie Sie den Internet-Zugang über einen vorkonfigurierten ISP konfigurieren

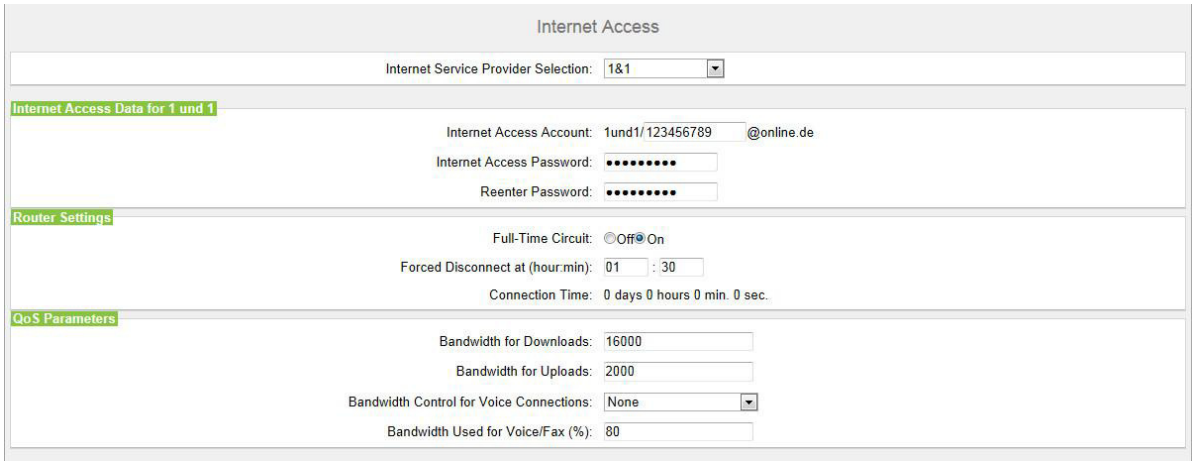
Voraussetzungen

- Sie befinden sich im Fenster **Konfiguration des Internetzugangs**.
- Die Internet-Zugangsdaten Ihres ISP liegen Ihnen vor (z. B. Benutzerkennung, Passwort, Bandbreite für Upload und Download).
- Optional: Die Daten für einen DynDNS-Account liegen Ihnen vor (Name, Passwort, Hostname, Domänenname des DynDNS-Providers)

Schritt für Schritt

1) Deaktivieren Sie das Kontrollkästchen **Kein Internet-Zugang**.

2) Aktivieren Sie das Optionsfeld **DSL am WAN Port des Mainboard direkt** und klicken Sie auf **OK & Weiter**.



3) Wählen Sie aus der Aufklappliste **Internet-Service-Provider-Auswahl** Ihren ISP aus.

4) Geben Sie im Bereich **Internet-Zugangsdaten für...** die Zugangsdaten ein, die Sie von ihrem ISP bekommen haben. Die Felder in diesem Bereich sind

providerabhängig. Achten Sie bei der Eingabe der Daten auf korrekte Groß- und Kleinschreibung.

5) Wählen Sie im Bereich **Router-Einstellungen** unter **Dauerverbindung** abhängig von Ihrem Tarifmodell eine der beiden folgenden Optionen aus:

- Haben Sie als Tarifmodell eine Flatrate, aktivieren Sie das Optionsfeld **An**. Legen Sie im Feld **Zwangstrennung um (Std:Min)** die Uhrzeit fest, zu der die Internet-Verbindung getrennt werden soll (z. B. 01:30). Zu dieser Zeit sollten keine Daten mit dem Internet ausgetauscht werden (z. B. Software-Downloads oder Internet-Telefonie).
- Haben Sie als Tarifmodell einen Zeittarif, aktivieren Sie das Optionsfeld **Aus**. Geben Sie im Feld **Automatisch trennen nach (Sekunden)** die Zeitdauer der Inaktivität an, nach der die Verbindung getrennt werden soll (z. B. 60 Sekunden).

6) Stellen Sie im Bereich **QoS-Parameter** die folgenden Werte ein:

a) Geben Sie in den Feldern **Bandbreite Download** und **Bandbreite Upload** die Bandbreite in kbit/s für den Download bzw. Upload ein, die Ihnen Ihr ISP zur Verfügung stellt.

b) Wenn Sie zusätzlich Internet-Telefonie nutzen wollen, wählen Sie aus der Aufklappliste **Bandbreitensteuerung für Sprach-Verbindungen** den Eintrag **Nur Upload** oder **Upload und Download** je nach Bedarf aus. Geben Sie im Feld **Bandbreite für Sprach-/Fax-Verbindungen (%)** in Prozent an, wieviel Bandbreite für Sprach- und Fax-Verbindungen reserviert werden soll (Standardwert: 80%).

7) Klicken Sie auf **OK & Weiter**. Sie werden zum Fenster **DynDNS-Account einrichten** geführt.

8) Wenn Sie VPN oder den Remote-Zugang nutzen wollen und keine öffentliche statische IP-Adresse haben, müssen Sie einen DynDNS-Account beantragt haben (z. B. bei dyndns.org) und ihn einrichten.

a) Wenn Ihr gewünschter DynDNS-Anbieter in der Aufklappliste **Domainname** enthalten ist, wählen Sie ihn aus der Liste aus (z. B. dyndns.org).

b) Wenn Ihr gewünschter DynDNS-Anbieter nicht in der Aufklappliste **Domainname** enthalten ist, aktivieren Sie das Kontrollkästchen **Benutzerdefinierte Domäne**. Geben Sie im Feld **Domainname** den gewünschten DynDNS-Anbieter ein und in dem Feld **Update-URL** die Update-URL des DynDNS-Anbieters. Der Aufbau dieser URL ist abhängig vom DynDNS-Anbieter. Zusätzlich sind kundenspezifische Parameter (im Beispiel *kursiv* markiert) zu ergänzen.

```
http://www.anydns.info/
update.php?user=<username>&password=<pass>&host=<doma
in>&ip=<ipaddr>
```

c) Geben Sie **Benutzername** und **Passwort** Ihres DynDNS-Accounts ein.

d) Geben Sie im Feld **Hostname** Ihren vom DynDNS-Anbieter zugeteilten Hostnamen ohne den Domänennamen ein, z. B. myhost. Ihr vollständiger Domänenname lautet dann z. B. myhost.dyndns.org.

e) Testen Sie den DynDNS-Account mit **Verbindung testen**.

f) Klicken Sie nach erfolgreichem Test auf **OK**.

g) Klicken Sie auf **OK & Weiter**.

9) Wenn Sie eine öffentliche statische IP-Adresse haben oder VPN oder den Remote-Zugang nicht nutzen wollen, klicken Sie auf **kein DynDNS**.

10) Klicken Sie auf **OK & Weiter**.

4.7.5.4 Wie Sie den Internet-Zugang über den Standard-ISP PPPoE konfigurieren

Voraussetzungen

- Sie befinden sich im Fenster **Konfiguration des Internetzugangs**.
- Folgende Internet-Zugangsdaten Ihres ISP liegen Ihnen vor:

Feld	Beschreibung	Wert vom ISP
IP-Parameter (nur bei fester IP-Adresse)		
Partner-IP-Adresse der PPP-Verbindung	IP-Adresse des Servers Ihres ISP.	
Lokale IP-Adresse der PPP-Verbindung	IP-Adresse, die Ihnen vom ISP für den Internet-Zugang zugeteilt wurde.	
Max. Datenpaketlänge (Byte)	Maximale Paketlänge in Byte, die für das IP-Protokoll gelten soll. Es sind Werte von 576 bis 1500 erlaubt.	
Authentifizierung (über PAP oder CHAP). PAP wird kaum noch verwendet, da die Authentifizierung unverschlüsselt ist.		
PPP-Benutzername	Benutzername für die PPP-Verbindung, der Ihnen vom ISP zugeteilt wurde.	
PAP-Authentifizierungsmode	Authentifizierungsmode für die PPP-Verbindung über PAP: **PAP-Client**, **PAP-Host** oder **nicht benutzt**.	
PAP-Kennwort	Kennwort für Authentifizierung durch PAP, das Ihnen vom ISP zugeteilt wurde.	
CHAP-Authentifizierungsmode	Authentifizierungsmode für die PPP-Verbindung über CHAP: **CHAP-Client**, **CHAP-Host**, **CHAP-Client und -Host** oder **nicht benutzt**.	
CHAP-Kennwort	Kennwort für Authentifizierung durch CHAP, das Ihnen vom ISP zugeteilt wurde.	
QoS-Parameter der Schnittstelle		
Bandbreite Download	Wert der gesamten Bandbreite in kbit/s für den Download vom ISP.	
Bandbreite Upload	Wert der gesamten Bandbreite in kbit/s für den Upload zum ISP.	

- Optional: Die Daten für einen DynDNS-Account liegen Ihnen vor (Name, Passwort, Hostname, Domänenname des DynDNS-Providers)

Schritt für Schritt

1) Deaktivieren Sie das Kontrollkästchen **Kein Internet-Zugang**.

2) Aktivieren Sie das Optionsfeld **DSL am WAN Port direkt** und klicken Sie auf **OK & Weiter**.

3) Wählen Sie aus der Aufklappliste **Internet-Service-Provider-Auswahl** den Standard ISP Typ **Provider-PPPoE** aus.

4) Aktivieren Sie im Bereich **IP-Parameter** das Kontrollkästchen **IP-Parameter** nur, wenn vom ISP eine Anpassung gefordert wird. Geben Sie in diesem Fall in den Feldern **Partner-IP-Adresse der PPP-Verbindung**, **Lokale IP-Adresse der PPP-Verbindung** und **Max. Datenpaketlänge (Byte)** die Werte ein, die Sie von Ihrem ISP bekommen haben. Wählen Sie aus der Aufklappliste **IP-Address-Aushandlung** den Eintrag **konfigurierte IP-Adresse nutzen** aus.

5) Wählen Sie im Bereich **Router-Einstellungen** unter **Dauerverbindung** abhängig von Ihrem Tarifmodell eine der beiden folgenden Optionen aus:

- Haben Sie als Tarifmodell eine Flatrate, aktivieren Sie das Optionsfeld **An**. Legen Sie im Feld **Zwangstrennung um (Std:Min)** die Uhrzeit fest, zu der die Internet-Verbindung getrennt werden soll (z. B. 01:30). Zu dieser Zeit sollten keine Daten mit dem Internet ausgetauscht werden (z. B. Software-Downloads oder Internet-Telefonie).
- Haben Sie als Tarifmodell einen Zeittarif, aktivieren Sie das Optionsfeld **Aus**. Geben Sie im Feld **Automatisch trennen nach (Sekunden)** die Zeitdauer der Inaktivität an, nach der die Verbindung getrennt werden soll (z. B. 60 Sekunden).

6) Die Einstellungen im Bereich **Authentifizierung** hängen davon ab, ob der ISP eine Authentifizierung über PPP fordert oder nicht.

- Authentifizierung wird vom ISP gefordert: Stellen Sie sicher, dass das Kontrollkästchen **PPP-Authentifizierung** aktiviert ist. Geben Sie als PPP-Benutzernamen den Internet-Zugangsnamen des ISP an. Der gebräuchliche Standard ist der Authentifizierungsmode **CHAP-Client**.
- Authentifizierung wird vom ISP nicht gefordert: Stellen Sie sicher, dass das Kontrollkästchen PPP-Authentifizierung deaktiviert ist.

7) Wenn Sie NAT nutzen wollen, aktivieren Sie im Bereich **Adressenübersetzung** das Kontrollkästchen **NAT** (standardmäßig aktiviert).

8) Stellen Sie im Bereich **QoS-Parameter der Schnittstelle** die folgenden Werte ein:

a) Geben Sie in den Feldern **Bandbreite Download** und **Bandbreite Upload** die Bandbreite in kbit/s für den Download bzw. Upload ein, die Ihnen Ihr ISP zur Verfügung stellt.

b) Wenn Sie zusätzlich Internet-Telefonie nutzen wollen, wählen Sie aus der Aufklappliste **Bandbreitensteuerung für Sprach-Verbindungen** den Eintrag **Nur Upload** oder **Upload und Download** je nach Bedarf aus. Geben Sie im Feld **Bandbreite für Sprach-/Fax-Verbindungen (%)** in Prozent an, wieviel Bandbreite für Sprach- und Fax-Verbindungen reserviert werden soll (Standardwert: 80%).

9) Klicken Sie auf **OK & Weiter**. Sie werden zum Fenster **DynDNS-Account einrichten** geführt.

10) Wenn Sie VPN oder den Remote-Zugang nutzen wollen und keine öffentliche statische IP-Adresse haben, müssen Sie einen DynDNS-Account beantragt haben (z. B. bei dyndns.org) und ihn einrichten.

a) Wenn Ihr gewünschter DynDNS-Anbieter in der Aufklappliste **Domainname** enthalten ist, wählen Sie ihn aus der Liste aus (z. B. dyndns.org).

b) Wenn Ihr gewünschter DynDNS-Anbieter nicht in der Aufklappliste **Domainname** enthalten ist, aktivieren Sie das Kontrollkästchen **Benutzerdefinierte Domäne**. Geben Sie im Feld **Domainname** den gewünschten DynDNS-Anbieter ein und in dem Feld **Update-URL** die Update-URL des DynDNS-Anbieters. Der Aufbau dieser URL ist

abhängig vom DynDNS-Anbieter. Zusätzlich sind kundenspezifische Parameter (im Beispiel *kursiv* markiert) zu ergänzen.

`http://www.anydns.info/update.php?user=<`*`username`*`>&password=<`*`pass`*`>&host=<`*`domain`*`>&ip=<`*`ipaddr`*`>`

c) Geben Sie **Benutzername** und **Passwort** Ihres DynDNS-Accounts ein.

d) Geben Sie im Feld **Hostname** Ihren vom DynDNS-Anbieter zugeteilten Hostnamen ohne den Domänennamen ein, z. B. myhost. Ihr vollständiger Domänenname lautet dann z. B. myhost.dyndns.org.

e) Testen Sie den DynDNS-Account mit **Verbindung testen**.

f) Klicken Sie nach erfolgreichem Test auf **OK**.

g) Klicken Sie auf **OK & Weiter**.

11) Wenn Sie eine öffentliche statische IP-Adresse haben oder VPN oder den Remote-Zugang nicht nutzen wollen, klicken Sie auf **kein DynDNS**.

12) Klicken Sie auf **OK & Weiter**.

4.7.5.5 Wie Sie den Internet-Zugang über einen Standard-ISP PPTP konfigurieren

Voraussetzungen

- Sie befinden sich im Fenster **Konfiguration des Internetzugangs**.
- Folgende Internet-Zugangsdaten Ihres ISP liegen Ihnen vor:

Feld	Beschreibung	Wert vom ISP
IP-Parameter (nur bei fester IP-Adresse)		
Partner-IP-Adresse der PPP-Verbindung	IP-Adresse des Servers Ihres ISP.	
Lokale IP-Adresse der PPP-Verbindung	IP-Adresse, die Ihnen vom ISP für den Internet-Zugang zugeteilt wurde.	
Max. Datenpaketlänge (Byte)	Maximale Paketlänge in Byte, die für das IP-Protokoll gelten soll. Es sind Werte von 576 bis 1500 erlaubt.	
PPTP-Parameter		
Lokale IP-Adresse der Kontrollverbindung	IP-Adresse, die Ihnen vom ISP für die PPTP-Verbindung zugeteilt wurde. Der voreingestellte Wert lautet 10.0.0.140.	
Partner-IP-Adresse der Kontrollverbindung	IP-Adresse des Servers Ihres ISP für die PPTP-Verbindung. Der voreingestellte Wert lautet 10.0.0.138.	
Partner-Netzmaske für die Kontrollverbindung	Netzmaske, die Ihnen vom ISP für die PPTP-Verbindung zugeteilt wurde. Der voreingestellte Wert lautet 255.255.255.248.	
Authentifizierung (über PAP oder CHAP). PAP wird kaum noch verwendet, da die Authentifizierung unverschlüsselt ist.		
PPP-Benutzername	Benutzername für die PPP-Verbindung, der Ihnen vom ISP zugeteilt wurde.	
PAP-Authentifizierungsmode	Authentifizierungsmode für die PPP-Verbindung über PAP: **PAP-Client**, **PAP-Host** oder **nicht benutzt**.	
PAP-Kennwort	Kennwort für Authentifizierung durch PAP, das Ihnen vom ISP zugeteilt wurde.	
CHAP-Authentifizierungsmode	Authentifizierungsmode für die PPP-Verbindung über CHAP: **CHAP-Client**, **CHAP-Host**, **CHAP-Client und -Host** oder **nicht benutzt**.	
CHAP-Kennwort	Kennwort für Authentifizierung durch CHAP, das Ihnen vom ISP zugeteilt wurde.	
QoS-Parameter der Schnittstelle		
Bandbreite Download	Wert der gesamten Bandbreite in kbit/s für den Download vom ISP.	
Bandbreite Upload	Wert der gesamten Bandbreite in kbit/s für den Upload zum ISP.	

- Optional: Die Daten für einen DynDNS-Account liegen Ihnen vor (Name, Passwort, Hostname, Domänenname des DynDNS-Providers)

Schritt für Schritt

1) Deaktivieren Sie das Kontrollkästchen **Kein Internet-Zugang**.

2) Aktivieren Sie das Optionsfeld **DSL am WAN Port direkt** und klicken Sie auf **OK & Weiter**.

3) Wählen Sie aus der Aufklappliste **Internet-Service-Provider-Auswahl** den Standard ISP Typ **Provider-PPTP** aus.

4) Aktivieren Sie im Bereich **IP-Parameter** das Kontrollkästchen **IP-Parameter** nur, wenn vom ISP eine Anpassung gefordert wird. Geben Sie in diesem Fall in den Feldern **Partner-IP-Adresse der PPP-Verbindung**, **Lokale IP-Adresse der PPP-Verbindung** und **Max. Datenpaketlänge (Byte)** die Werte ein, die Sie von Ihrem ISP bekommen haben. Wählen Sie aus der Aufklappliste **IP-Address-Aushandlung** den Eintrag **konfigurierte IP-Adresse nutzen** aus.

5) Geben Sie in dem Bereich **PPTP-Parameter** die Werte ein, die Sie von Ihrem ISP bekommen haben.

6) Wenn Sie als Tarifmodell einen Zeittarif haben, aktivieren Sie das Kontrollkästchen **Short-Hold-Modus**. Geben Sie im Feld **Short-Hold-Zeit (s)** die Zeitdauer der Inaktivität an, nach der die Verbindung getrennt werden soll (z. B. 60 Sekunden).

7) Die Einstellungen im Bereich **Authentifizierung** hängen davon ab, ob der ISP eine Authentifizierung über PPP fordert oder nicht.

- Authentifizierung wird vom ISP gefordert: Stellen Sie sicher, dass das Kontrollkästchen **PPP-Authentifizierung** aktiviert ist. Geben Sie als PPP-Benutzernamen den Internet-Zugangsnamen des ISP an. Treffen Sie die PAP- und CHAP-Einstellungen, wie Sie sie von Ihrem ISP zugeteilt bekommen haben.
- Authentifizierung wird vom ISP nicht gefordert: Stellen Sie sicher, dass das Kontrollkästchen PPP-Authentifizierung deaktiviert ist.

8) Wenn Sie NAT nutzen wollen, aktivieren Sie im Bereich **Adressenübersetzung** das Kontrollkästchen **NAT** (standardmäßig aktiviert).

9) Stellen Sie im Bereich **QoS-Parameter der Schnittstelle** die folgenden Werte ein:

a) Geben Sie in den Feldern **Bandbreite Download** und **Bandbreite Upload** die Bandbreite in kbit/s für den Download bzw. Upload ein, die Ihnen Ihr ISP zur Verfügung stellt.

b) Wenn Sie zusätzlich Internet-Telefonie nutzen wollen, wählen Sie aus der Aufklappliste **Bandbreitensteuerung für Sprach-Verbindungen** den Eintrag **Nur Upload** oder **Upload und Download** je nach Bedarf aus. Geben Sie im Feld **Bandbreite für Sprach-/Fax-Verbindungen (%)** in Prozent an, wieviel Bandbreite für Sprach- und Fax-Verbindungen reserviert werden soll (Standardwert: 80%).

10) Klicken Sie auf **OK & Weiter**. Sie werden zum Fenster **DynDNS-Account einrichten** geführt.

11) Wenn Sie VPN oder den Remote-Zugang nutzen wollen und keine öffentliche statische IP-Adresse haben, müssen Sie einen DynDNS-Account beantragt haben (z. B. bei dyndns.org) und ihn einrichten.

a) Wenn Ihr gewünschter DynDNS-Anbieter in der Aufklappliste **Domainname** enthalten ist, wählen Sie ihn aus der Liste aus (z. B. dyndns.org).

b) Wenn Ihr gewünschter DynDNS-Anbieter nicht in der Aufklappliste **Domainname** enthalten ist, aktivieren Sie das Kontrollkästchen **Benutzerdefinierte Domäne**. Geben Sie im Feld **Domainname** den gewünschten DynDNS-Anbieter ein und in dem Feld **Update-URL** die Update-URL des DynDNS-Anbieters. Der Aufbau dieser URL ist abhängig vom DynDNS-Anbieter. Zusätzlich sind kundenspezifische Parameter (im Beispiel *kursiv* markiert) zu ergänzen.

`http://www.anydns.info/update.php?user=<`*`username`*`>&password=<`*`pass`*`>&host=<`*`domain`*`>&ip=<`*`ipaddr`*`>`

c) Geben Sie **Benutzername** und **Passwort** Ihres DynDNS-Accounts ein.

d) Geben Sie im Feld **Hostname** Ihren vom DynDNS-Anbieter zugeteilten Hostnamen ohne den Domänennamen ein, z. B. myhost. Ihr vollständiger Domänenname lautet dann z. B. myhost.dyndns.org.

e) Testen Sie den DynDNS-Account mit **Verbindung testen**.

f) Klicken Sie nach erfolgreichem Test auf **OK**.

g) Klicken Sie auf **OK & Weiter**.

12) Wenn Sie eine öffentliche statische IP-Adresse haben oder VPN oder den Remote-Zugang nicht nutzen wollen, klicken Sie auf **kein DynDNS**.

13) Klicken Sie auf **OK & Weiter**.

4.7.5.6 Wie Sie den Internet-Zugang deaktivieren

Voraussetzungen

- Sie befinden sich im Fenster **Konfiguration des Internetzugangs**.

Schritt für Schritt

1) Lassen Sie das Kontrollkästchen **Kein Internet-Zugang** aktiviert.

2) Klicken Sie auf **OK & Weiter**.

4.7.6 Internet-Telefonie

Im Fenster **Provider-Konfiguration und -Aktivierung für Internet-Telefonie** konfigurieren Sie die Internet-Telefonie. Sie können vorkonfigurierte oder neue Internet-Telefonie-Service-Provider (ITSP) konfigurieren. Für jeden ITSP können

Sie einen oder mehrere Accounts konfigurieren. Es können bis zu 4 ITSP gleichzeitig aktiv sein.

Sie haben folgende Möglichkeiten:

- **Vordefinierten ITSP konfigurieren**
  Sie können vordefinierte ITSP-Vorlagen verwenden. Dazu werden in diese Vorlage die eigenen Zugangsdaten und Rufnummern eingetragen und diese anschließend aktiviert.
- **Neuen ITSP konfigurieren**
  Sie können auch neue ITSP hinzufügen und aktivieren.
  Einen neuen ITSP zu konfigurieren ist nur in seltenen Fällen nötig und sehr aufwändig. Deshalb wird diese Möglichkeit nicht in der Erstinstallation beschrieben. Genauere Informationen finden Sie im Kapitel *Konfiguration eines ITSP*.
- **Internet-Telefonie deaktivieren**
  Sie können die Internet-Telefonie deaktivieren.

INFO: Einrichtebeispiele finden Sie im wiki unter http://wiki.unify.com/images/1/1e/OSBiz_V1_Configuration_for_ITSP.pdf

---

Zuordnung der ITSP-Rufnummern

- Bei einem **Internet-Telefonie-Teilnehmeranschluss** stellt der ITSP Einzelrufnummern zur Verfügung, z. B. 70005555, 70005556, ... Diese Einzelrufnummern werden anschließend den internen Rufnummern der Teilnehmer manuell zugeordnet.
- Bei einem **Internet-Telefonie-Anlagenanschluss** stellt der ITSP ein Rufnummernband (Rufnummernbereich) zur Verfügung, z. B. (+49) 89 7007-100 bis (+49) 89 7007-147. Die Rufnummern aus dem Rufnummernband werden anschließend den internen Rufnummern der Teilnehmer manuell zugeordnet.

Die beiden Anschlussarten können kombiniert werden.

Alternativ können für beide Anschlussarten die ITSP-Rufnummern bei der Teilnehmer-Konfiguration als Durchwahlrufnummern der Teilnehmer eingetragen werden.

interne Rufnummer	Name	DuWa
100	Andreas Richter	897007100
101	Susanne Mueller	897007101
102	Buddy Miller	897007102
104	Juan Martinez	70005555
105	Emilio Carrara	70005556

Somit ergeben sich die ITSP-Rufnummern aus der eingerichteten Anlagenrufnummer (z. B. Länderkennzahl 49) und den eingetragenen

Durchwahlnummern im Langformat. Das hat Vorteile bei der Wahlbewertung und dem Call-Management, auch in einem Netzverbund. So ist der ITSP-Anschluss z. B. durchwahlfähig zu einem anderen Knoten.

Ein weiterer Amtsanschluss über ISDN ist in diesem Fall nur eingeschränkt möglich (sinnvoll z. B. für Notrufe).

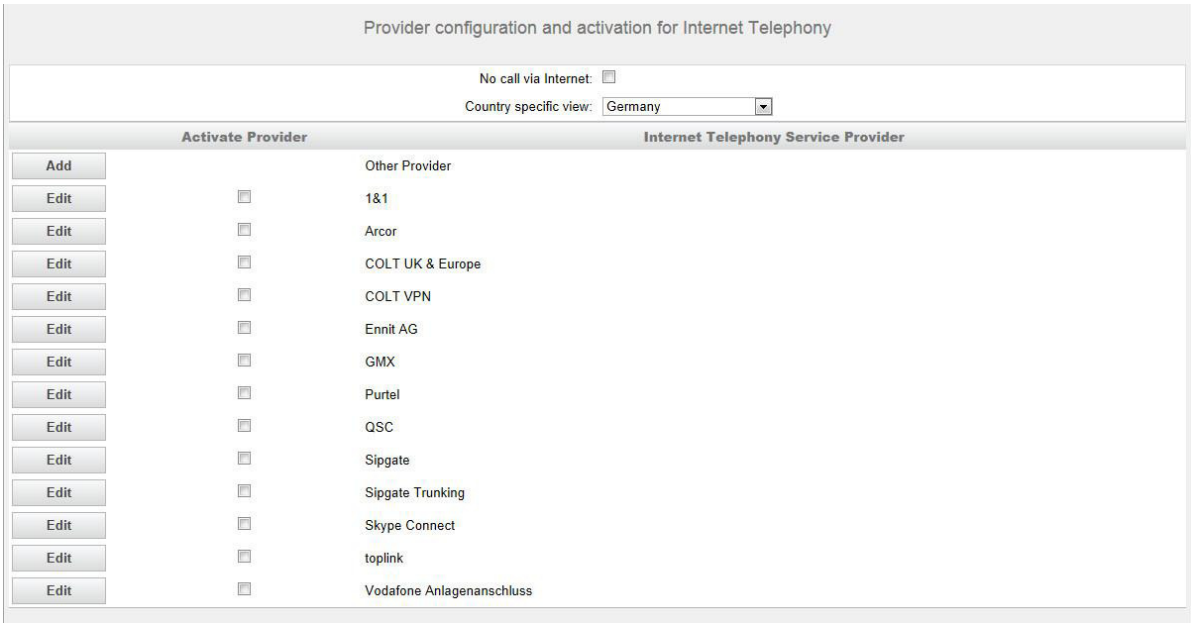
4.7.6.1 Wie Sie einen vordefinierten ITSP konfigurieren

Voraussetzungen

- Sie befinden sich im Fenster **Provider-Konfiguration und -Aktivierung für Internet-Telefonie**.
- Die Verbindung zum Internet ist betriebsbereit.
- Die Internet-Telefonie-Zugangsdaten Ihres ITSP liegen Ihnen vor (z. B. Benutzerkennung, Passwort, Internet-Telefonie-Rufnummern).

Schritt für Schritt

1) Deaktivieren Sie das Kontrollkästchen **Keine Telefonie über Internet**. Es wird Ihnen eine landesabhängige Liste der möglichen ITSP angezeigt. Die Liste enthält die für das gewählte Land vordefinierten ITSP und die eventuell bereits angelegten ITSP.



2) Wenn Sie das voreingestellte Land ändern möchten, wählen Sie aus der Aufklappliste **Länderspezifische Ansicht** das gewünschte Land aus. Es werden die für das gewählte Land möglichen ITSP angezeigt.

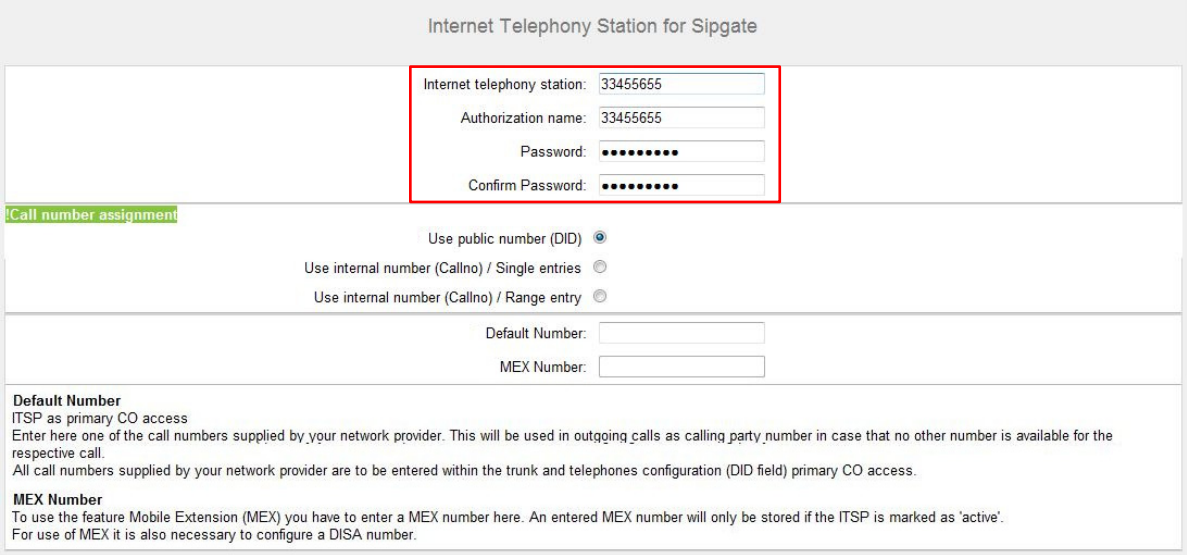
3) Klicken Sie bei Bedarf auf **Status anzeigen**, um abzufragen, welche ITSP bereits aktiviert sind und welche Internet-Telefonie-Teilnehmer unter dem jeweiligen ITSP bereits eingerichtet sind. Maximal können Sie vier ITSP aktivieren. Klicken Sie anschließend auf **OK**.

4) Klicken Sie in der Zeile des entsprechenden ITSP auf **Bearbeiten**, um einen vordefinierten ITSP zu konfigurieren.

5) Aktivieren Sie das Kontrollkästchen **Provider aktivieren**.

6) Klicken Sie auf **OK & Weiter**.

7) Klicken Sie auf **Hinzufügen**, um Ihre ITSP-Accounts mit den dazugehörigen Internet-Telefonie-Rufnummern zu konfigurieren. Die Felder, die Ihnen anschließend angezeigt werden, sind providerabhängig.



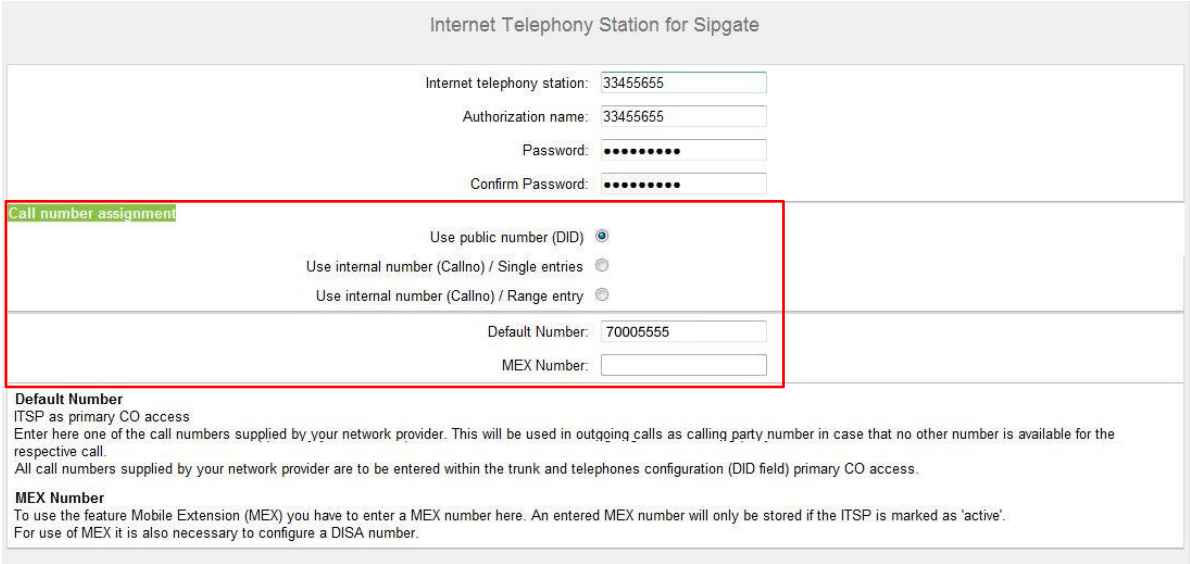
8) Geben im Feld **Internet-Telefonie-Teilnehmer** die Zugangsdaten Ihres Accounts ein. Die Daten haben Sie von Ihrem ITSP erhalten. Je nach ITSP werden hierfür unterschiedliche Bezeichnungen verwendet, wie z. B. SIP-User, SIP-Nutzer, SIP-ID.

9) Geben Sie im Feld **Autorisierungsname** den Autorisierungsnamen ein. Die Daten haben Sie von Ihrem ITSP erhalten. Haben Sie keinen Autorisierungsnamen erhalten, geben Sie die gleichen Daten wie unter **Internet-Telefonie-Teilnehmer** ein.

10) Geben Sie in den Feldern **Neues Kennwort** und **Kennwort wiederholen** das Kennwort an, dass Sie vom ITSP erhalten haben. Je nach ITSP werden hierfür unterschiedliche Bezeichnungen verwendet, wie z. B. SIP-Passwort oder SIP-Kennwort.

11) Zuordnung der Internet-Telefonie-Rufnummern - Möglichkeit 1:

Öffentliche Rufnummer (DuWa): die Internet-Telefonie-Rufnummern Ihres Internet-Telefonie-Teilnehmeranschlusses oder Internet-Telefonie-Anlagenanschlusses werden nicht hier bei der ITSP-Konfiguration, sondern bei der Teilnehmer-Konfiguration in den Feldern **DuWa** eingetragen.



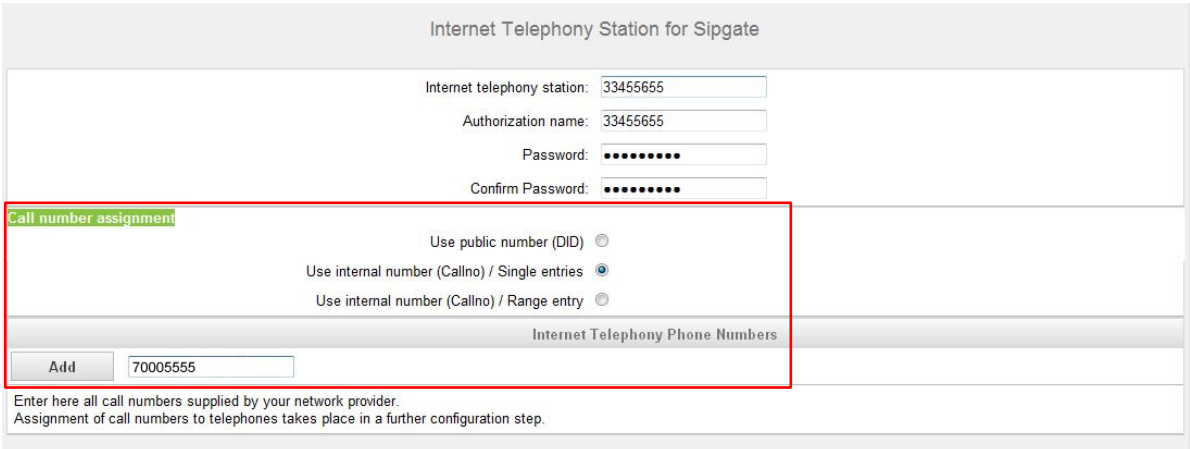
a) Wählen Sie im Bereich **Rufnummer assignment** das Optionsfeld **Öffentliche Rufnummer (DuWa)** aus.

b) Geben Sie unter **Standard-Rufnummer** die Rufnummer ein, die bei gehenden Anrufen für Teilnehmer verwendet werden soll, die keine eigene Rufnummer haben.

c) Falls Ihr ITSP das Leistungsmerkmal "Mobile Extension (MEX)" unterstützt, tragen Sie unter **MEX-Nummer** die vom ITSP zur Verfügung gestellte MEX-Nummer ein (8-stellig, nur Ziffern).

12) Zuordnung der Internet-Telefonie-Rufnummern - Möglichkeit 2:

Interne Nummer (Rufnr.) verwenden / Einzeleinträge: Sie haben einen Internet-Telefonie-Teilnehmeranschluss und als Internet-Telefonie-Rufnummern Einzelrufnummern erhalten (z. B. 70005555, 70005556,...). Diese Einzelrufnummern ordnen Sie anschließend den internen Rufnummern der Teilnehmer zu.



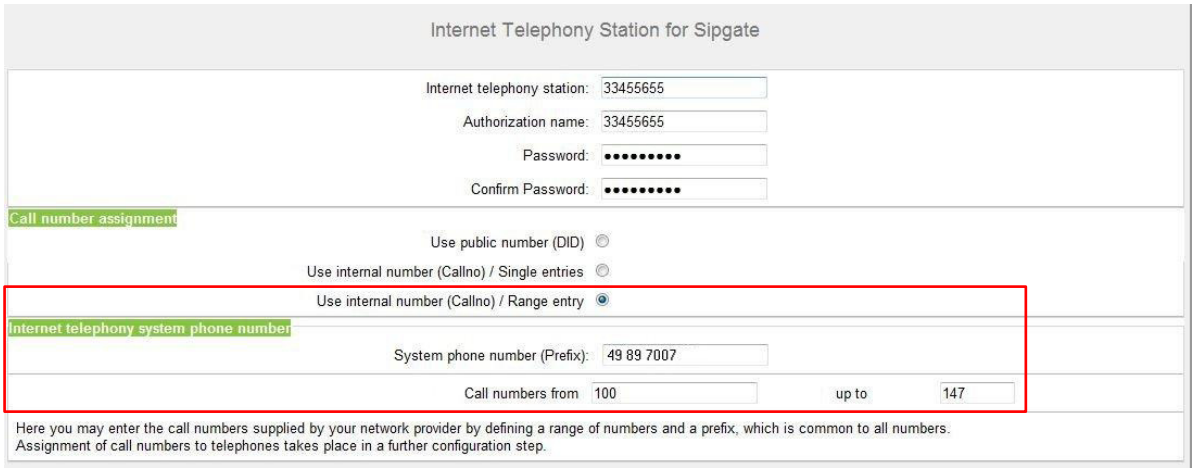
a) Wählen Sie im Bereich **Rufnummer assignment** das Optionsfeld **Interne Nummer (Rufnr.) verwenden / Einzeleinträge** aus.

b) Geben Sie im Bereich **Internet-Telefonie-Teilnehmerrufnummern** im Feld neben der Schaltfläche **Hinzufügen** eine der vom ITSP mitgeteilten Internet-Telefonie-Rufnummern ein und klicken Sie auf **Hinzufügen**.

c) Wenn Sie dem Account weitere Internet-Telefonie-Rufnummern zuordnen wollen, wiederholen Sie Schritt b).

13) Zuordnung der Internet-Telefonie-Rufnummern - Möglichkeit 3:

Interne Nummer (Rufnr.) verwenden / Bereichseintrag: Sie haben einen Internet-Telefonie-Anlagenanschluss und als Internet-Telefonie-Rufnummern ein Rufnummernband erhalten, z. B. (+49) 89 7007-100 bis (+49) 89 7007-147. Die Rufnummern aus dem Rufnummernband ordnen Sie anschließend den internen Rufnummern der Teilnehmer zu.



a) Wählen Sie im Bereich **Rufnummer assignment** das Optionsfeld **Interne Nummer (Rufnr.) verwenden / Bereichseintrag** aus.

b) Geben Sie unter **Anlagenrufnummer (Präfix)** die Anlagenrufnummer ein.

c) Geben Sie in den Feldern **Durchwahlband von** und **bis** das gewünschte Durchwahlband für den Internet-Telefonie-Teilnehmer ein. Standardmäßig ist 100 - 147 eingetragen.

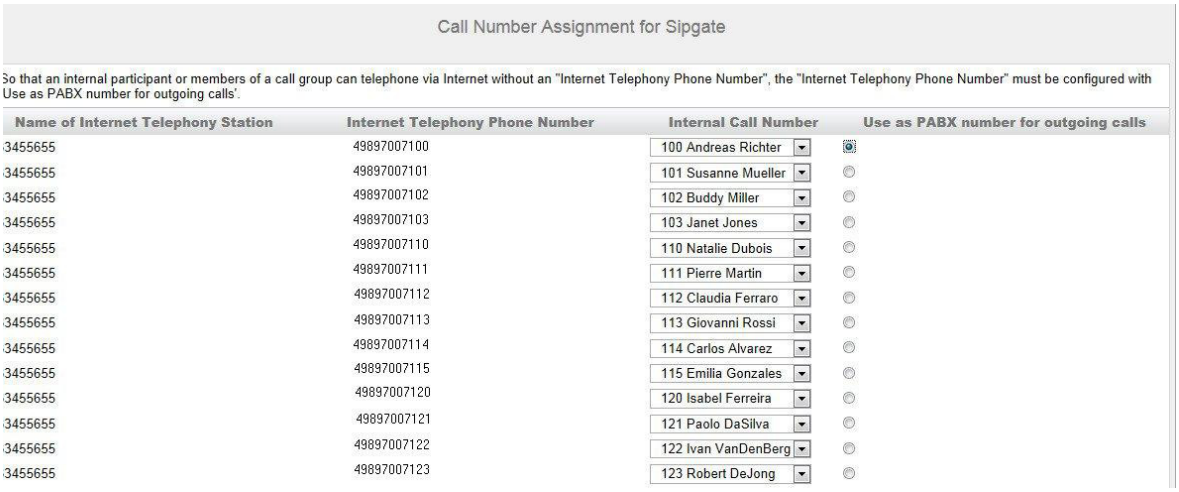
14) Klicken Sie auf **OK & Weiter**.

15) Wenn Sie weitere Accounts mit den dazugehörigen Internet-Telefonie-Rufnummern einrichten möchten, wiederholen Sie die Schritte 7 bis 14.

16) Klicken Sie auf **OK & Weiter**. Sie sehen eine Übersicht, welche Internet-Telefonie-Rufnummern welchen Accounts zugeordnet sind.

17) Ordnen Sie allen Internet-Telefonie-Rufnummern jeweils einer internen Rufnummer eines Teilnehmers zu.

Dieser Schritt entfällt, wenn Sie für die Zuordnung der Internet-Telefonie-Rufnummern die Möglichkeit 1 gewählt haben. Die Zuordnung treffen Sie in diesem Fall bei der Teilnehmer-Konfiguration im Feld **DuWa**.



Call Number Assignment for Sipgate

So that an internal participant or members of a call group can telephone via Internet without an "Internet Telephony Phone Number", the "Internet Telephony Phone Number" must be configured with Use as PABX number for outgoing calls'.

Name of Internet Telephony Station	Internet Telephony Phone Number	Internal Call Number	Use as PABX number for outgoing calls
3455655	49897007100	100 Andreas Richter	◉
3455655	49897007101	101 Susanne Mueller	○
3455655	49897007102	102 Buddy Miller	○
3455655	49897007103	103 Janet Jones	○
3455655	49897007110	110 Natalie Dubois	○
3455655	49897007111	111 Pierre Martin	○
3455655	49897007112	112 Claudia Ferraro	○
3455655	49897007113	113 Giovanni Rossi	○
3455655	49897007114	114 Carlos Alvarez	○
3455655	49897007115	115 Emilia Gonzales	○
3455655	49897007120	120 Isabel Ferreira	○
3455655	49897007121	121 Paolo DaSilva	○
3455655	49897007122	122 Ivan VanDenBerg	○
3455655	49897007123	123 Robert DeJong	○

a) Wählen Sie in der entsprechenden Zeile aus der Aufklappliste **interne Rufnummer** eine interne Rufnummer aus.

b) Sollen Teilnehmer ohne Internet-Telefonie-Rufnummer oder Mitglieder einer Rufgruppe externe Telefonate über das Internet führen dürfen, muss das Optionsfeld **Als gehende Anlagenrufnummer verwenden** aktiviert sein. Das Optionsfeld kann ausschließlich bei einer einzigen Internet-Telefonie-Rufnummer aktiviert sein.

18) Klicken Sie auf **OK & Weiter**. Hier sehen Sie nochmals die Liste der vordefinierten und neu hinzugefügten ITSP. Aktivierte ITSP sind in der Spalte **Provider aktivieren** mit einem Häkchen markiert. Mit **Restart ITSP** können Sie sich bei Verbindungsproblemen bei bereits aktivierten ITSP neu registrieren

19) Klicken Sie auf **OK & Weiter**.

20) Geben Sie im Feld **Upstream bis zu (Kbit/s)** den Wert der Upload-Geschwindigkeit Ihrer Internet-Verbindung ein. Nicht zu verwechseln mit der Download-Geschwindigkeit!

INFO: Im Feld **Anzahl simultaner Internet-Telefongespräche** wird Ihnen die Anzahl der gleichzeitig zu führenden Internet-Telefongespräche angezeigt. Wenn sich auf Grund der Netzauslastung die Gesprächsqualität verschlechtert, müssen Sie die Anzahl reduzieren.

---

21) Klicken Sie auf **OK & Weiter**.

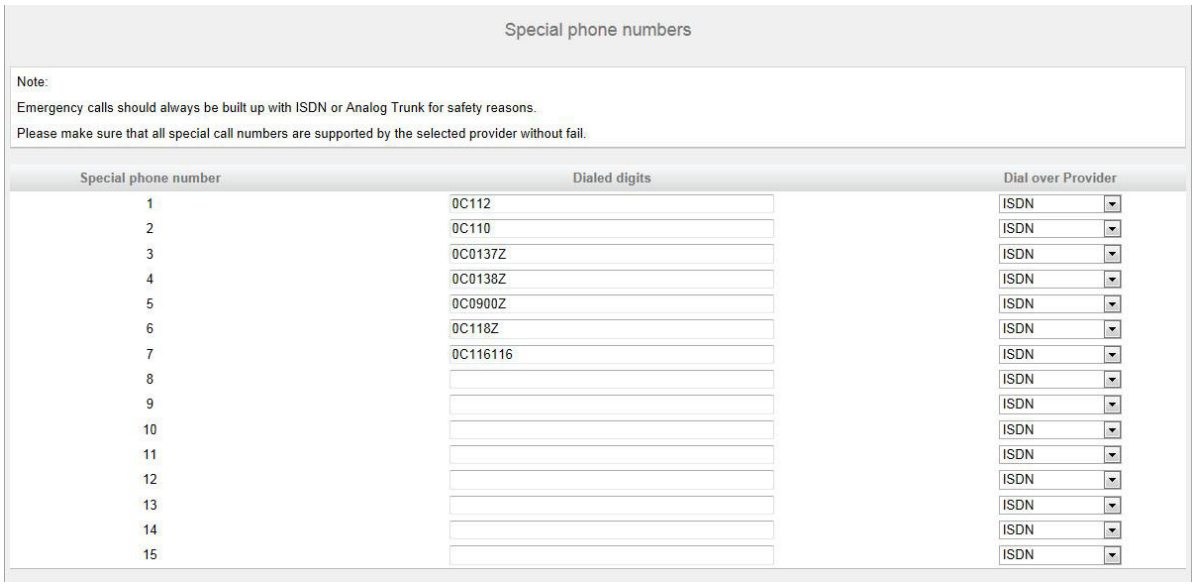
22) Falls Sie bei der Einrichtung Ihres Internet-Zugangs die Dauerverbindung noch nicht aktiviert haben, können Sie das hier nachholen. Ohne Dauerverbindung können Sie keine Anrufe über das Internet empfangen. Ist die Dauerverbindung bereits eingerichtet, erscheinen die unter a) bis c) beschriebenen Felder nicht.

a) Aktivieren Sie unter **Dauerverbindung** das Optionsfeld **An**.

b) Legen Sie im Feld **Zwangstrennung um (Std:Min)** die Uhrzeit fest, zu der die Internet-Verbindung getrennt werden soll (z. B. 04:59).

c) Klicken Sie auf **OK & Weiter**.

23) Tragen Sie in der Spalte **Gewählte Ziffern** die gewünschten Sonderrufnummern ein.



Folgende Rufnummerneinträge sind gültig:

0 bis 9: erlaubte Ziffern

-: Feldtrennzeichen

X: beliebige Ziffer zwischen 0 bis 9

N: beliebige Ziffer zwischen 2 bis 9

Z: eine oder mehrere Ziffern folgen bis Wahlende

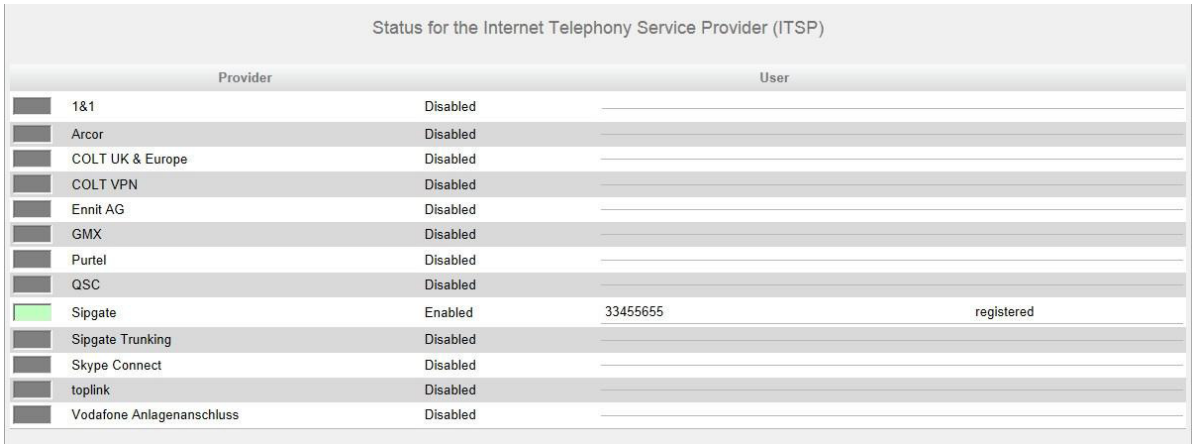
C: simulierter Wählton (kann max. 3 mal eingetragen werden)

24) Wählen Sie in der Spalte **Wählen über Provider** aus, ob die Sonderrufnummer über ISDN oder über einen ITSP gewählt werden soll. Es werden nur aktive ITSP angezeigt.

INFO: Stellen Sie sicher, dass Notrufnummern immer gewählt werden können. Falls Notrufnummern über einen Internet-Telefonie-Service-Provider gewählt werden sollen, muss der ITSP dies unterstützen.

---

25) Klicken Sie auf **OK & Weiter**. Es wird Ihnen der Status der ITSP angezeigt.



Grün markiert sind ITSP, die eingerichtet und an denen Sie bereits registriert sind.

Orange markiert sind ITSP, die eingerichtet und an denen Sie noch nicht registriert sind.

26) Klicken Sie auf **Weiter** und anschließend auf **Beenden**.

4.7.6.2 Wie Sie die Internet-Telefonie deaktivieren

Voraussetzungen

- Sie befinden sich im Fenster **Provider-Konfiguration und -Aktivierung für Internet-Telefonie**.

Schritt für Schritt

1) Lassen Sie das Kontrollkästchen **Keine Telefonie über Internet** aktiviert.

2) Klicken Sie zweimal auf **OK & Weiter**.

4.7.7 Teilnehmer

In den Fenstern **Teilnehmer auswählen - ...** konfigurieren Sie die an dem Kommunikationssystem angeschlossenen Teilnehmer.

Gehen Sie folgendermaßen vor:

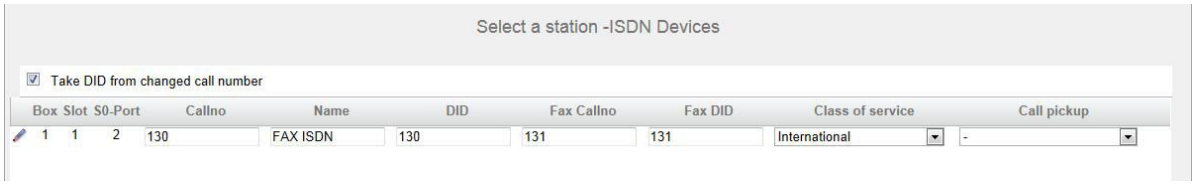
1. ISDN-Teilnehmer konfigurieren
   ISDN-Teilnehmer sind z. B. ISDN-Telefone oder ISDN-Faxgeräte. ISDN-Teilnehmer können Sie nur konfigurieren, wenn Sie eine S_0-Schnittstelle als internen S_0-Anschluss konfiguriert haben.
2. Analoge Teilnehmer konfigurieren
   Analoge Teilnehmer sind z. B. analoge Telefone oder analoge Faxgeräte.
3. UP0-Teilnehmer konfigurieren
   UP0-Teilnehmer sind Systemtelefone wie OpenStage 60 T.

4. DECT-Teilnehmer konfigurieren
   DECT-Teilnehmer sind Cordless/DECT-Telefone. DECT-Teilnehmer können Sie nur konfigurieren, wenn eine oder mehrere Cordless-Basisstationen angeschlossen und die DECT-Telefone dort angemeldet sind. Die Konfiguration der Basisstation wird mit dem Manager E durchgeführt. Genauere Informationen zur Konfiguration von Cordless siehe *Konfiguration der integrierten Cordless-Lösung*
5. IP- und SIP-Teilnehmer konfigurieren
   IP-Teilnehmer und SIP-Teilenehmer sind z. B. LAN-Telefone oder WLAN-Telefone.

4.7.7.1 Wie Sie ISDN-Teilnehmer konfigurieren

Voraussetzungen

- Sie befinden sich im Fenster **Teilnehmer auswählen - ISDN-Endgeräte**.
- Die S_0-Anschlüsse, an denen die ISDN-Telefone angeschlossen sind, müssen als interner S_0-Anschluss eingerichtet sein.



Schritt für Schritt

1) Wenn sich die Durchwahlnummer des Teilnehmers von seiner Rufnummer unterscheiden soll, geben Sie in der Zeile des gewünschten Teilnehmers unter **DuWa** eine Durchwahl-Nummer für den Teilnehmer ein:

- nur bei Anlagenanschluss:
  Klicken Sie in das gewünschte Feld und geben Sie über die Tastatur die Durchwahlnummer ein. Die Durchwahlnummer kann auch mit der internen Rufnummer identisch sein.
- nur bei Mehrgeräteanschluss:
  Wählen Sie in dem gewünschten Feld über die Aufklappliste eine MSN aus. Der Teilnehmer kann z. B. von intern über die interne Rufnummer 101 und von extern über die MSN 654321 erreicht werden.
- bei Anlagenanschluss und Mehrgeräteanschluss:
  Wählen Sie in dem gewünschten Feld über die Aufklappliste den Eintrag **xxx - änderbar** aus (xxx steht für die interne Rufnummer) und geben Sie über die Tastatur die Durchwahlnummer ein oder wählen Sie über die Aufklappliste eine MSN aus.

2) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Rufnr** eine interne Rufnummer für den Teilnehmer ein. Sie können die vorbelegte

Rufnummer verwenden oder eine andere, noch nicht belegte Rufnummer vergeben.

3) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Name** einen Namen in der Form `Nachname, Vorname` oder `Vorname Nachname` ein.

> ***INFO:*** Der Name kann aus bis zu 16 Zeichen bestehen, darf aber keine Umlaute oder Sonderzeichen enthalten.

4) Wenn für den Teilnehmer eine Faxbox eingerichtet werden soll (nutzbar z. B. mit den UC Clients **myPortal for Desktop** oder **myPortal for Outlook**), gehen Sie folgendermaßen vor:

a) Geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax Rufnr** die gewünschte interne Fax-Rufnummer ein, unter der der Teilnehmer von intern Faxnachrichten empfangen kann.

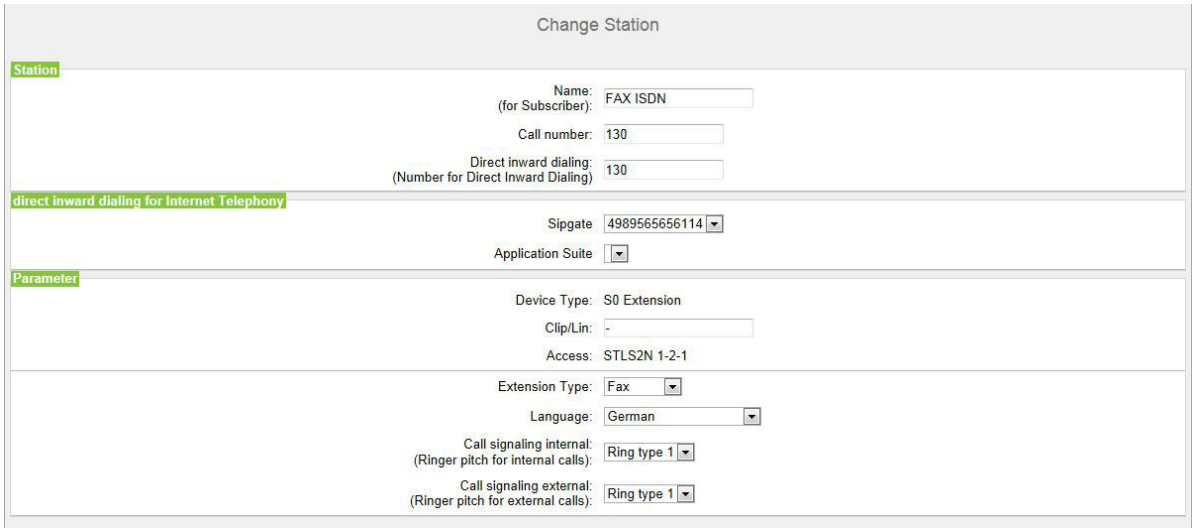
b) Wenn für die Faxbox eine Durchwahlnummer konfiguriert werden soll, geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax Durchwahl** die gewünschte externe Fax-Rufnummer ein, unter der der Teilnehmer von extern Faxnachrichten empfangen kann.

5) Wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Berechtigung** die gewünschte Berechtigungsgruppe aus.

6) Um den Teilnehmer in eine Anrufübernahmegruppe aufzunehmen, wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Anrufübernahme** eine Anrufübernahmegruppe aus.

7) Führen Sie die unter diesem Schritt beschriebenen Einstellungen nur bei Bedarf durch:

a) Klicken Sie in der Zeile des gewünschten ISDN-Teilnehmers auf das Stiftsymbol **Bearbeiten**.



b) Geben Sie im Feld **Clip/Lin** eine Rufnummer ein (Durchwahlnummer oder MSN), die beim einem externen Anruf im Display des Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird.

INFO: Dieses Leistungsmerkmal muss vom Netzanbieter freigegeben sein.

c) Wählen Sie aus der Aufklappliste **Stationstyp** den Typ des ISDN-Endgeräts aus.

d) Wählen Sie im Bereich **Durchwahl für Internet-Telefonie** aus einer Aufklappliste eine Durchwahlnummer aus. Für jeden aktiven ITSP wird Ihnen eine Aufklappliste angezeigt.

INFO: Das Feld **Durchwahl für Internet-Telefonie** ist nicht sichtbar, wenn die Internet-Telefonie nicht eingerichtet oder kein Internet-Telefonie-Service-Provider aktiviert ist.

e) Weisen Sie aus der Aufklappliste **Rufsignalisierung intern** dem Teilnehmer eine von insgesamt acht möglichen akustischen Rufsignalisierungen für interne Anrufe zu. Dadurch sendet der Teilnehmer anderen internen Teilnehmern einen veränderten Rufton, durch den er von anderen Teilnehmern unterschieden werden kann (Standard: Rufart 1).

f) Weisen Sie aus der Aufklappliste **Rufsignalisierung extern** dem Teilnehmer eine von insgesamt drei möglichen akustischen Rufsignalisierungen für externe Anrufe zu (Standard: Rufart 1).

g) Klicken Sie auf **OK & Weiter**.

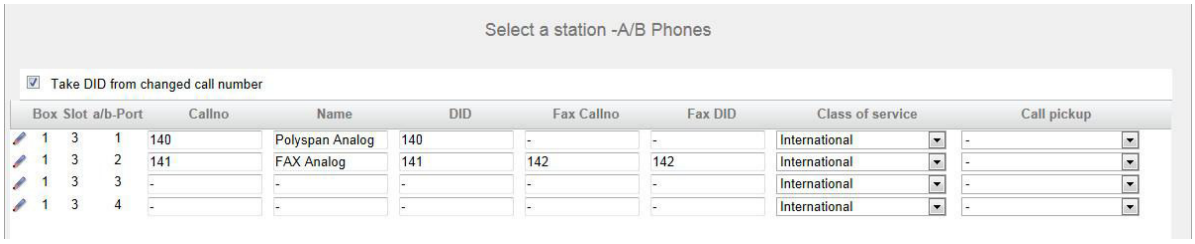
8) Wenn Sie weitere ISDN-Teilnehmer einrichten möchten, klicken Sie auf **Daten speichern** und wiederholen Sie die Schritte 1 bis 7.

9) Klicken Sie auf **OK & Weiter**.

4.7.7.2 Wie Sie analoge Teilnehmer konfigurieren

Voraussetzungen

- Sie befinden sich im Fenster **Teilnehmer auswählen - A/B-Endgeräte**.
- Ein Mainboard oder eine Baugruppe mit analogen Schnittstellen ist vorhanden.



Schritt für Schritt

1) Wenn sich die Durchwahlnummer des Teilnehmers von seiner Rufnummer unterscheiden soll, geben Sie in der Zeile des gewünschten Teilnehmers unter **DuWa** eine Durchwahl-Nummer für den Teilnehmer ein:

- nur bei Anlagenanschluss:

  Klicken Sie in das gewünschte Feld und geben Sie über die Tastatur die Durchwahlnummer ein. Die Durchwahlnummer kann auch mit der internen Rufnummer identisch sein.

- nur bei Mehrgeräteanschluss:

  Wählen Sie in dem gewünschten Feld über die Aufklappliste eine MSN aus. Der Teilnehmer kann z. B. von intern über die interne Rufnummer 101 und von extern über die MSN 654321 erreicht werden.

- bei Anlagenanschluss und Mehrgeräteanschluss:

  Wählen Sie in dem gewünschten Feld über die Aufklappliste den Eintrag **xxx - änderbar** aus (xxx steht für die interne Rufnummer) und geben Sie über die Tastatur die Durchwahlnummer ein oder wählen Sie über die Aufklappliste eine MSN aus.

2) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Rufnr** eine interne Rufnummer für den Teilnehmer ein. Sie können die vorbelegte Rufnummer verwenden oder eine andere, noch nicht belegte Rufnummer vergeben.

3) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Name** einen Namen in der Form `Nachname, Vorname` oder `Vorname Nachname` ein.

INFO: Der Name kann aus bis zu 16 Zeichen bestehen, darf aber keine Umlaute oder Sonderzeichen enthalten.

---

4) Wenn für den Teilnehmer eine Faxbox eingerichtet werden soll (nutzbar z. B. mit den UC Clients **myPortal for Desktop** oder **myPortal for Outlook**), gehen Sie folgendermaßen vor:

a) Geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax Rufnr** die gewünschte interne Fax-Rufnummer ein, unter der der Teilnehmer von intern Faxnachrichten empfangen kann.

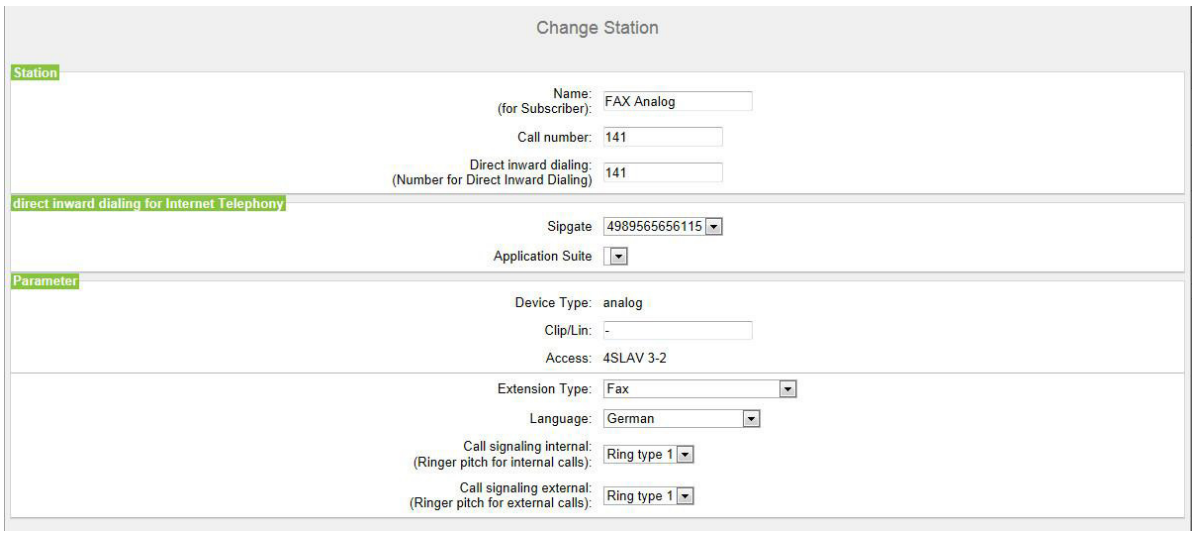
b) Wenn für die Faxbox eine Durchwahlnummer konfiguriert werden soll, geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax DuWa** die gewünschte externe Fax-Rufnummer ein, unter der der Teilnehmer von extern Faxnachrichten empfangen kann.

5) Wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Berechtigung** die gewünschte Berechtigungsgruppe aus.

6) Um den Teilnehmer in eine Anrufübernahmegruppe aufzunehmen, wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Anrufübernahme** eine Anrufübernahmegruppe aus.

7) Führen Sie die unter diesem Schritt beschriebenen Einstellungen nur bei Bedarf durch:

a) Klicken Sie in der Zeile des gewünschten analogen Teilnehmers auf das Stiftsymbol **Bearbeiten**.



b) Geben Sie im Feld **Clip/Lin** eine Rufnummer ein (Durchwahlnummer oder MSN), die beim einem externen Anruf im Display des Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird.

INFO: Dieses Leistungsmerkmal muss vom Netzanbieter freigegeben sein.

---

c) Wählen Sie aus der Aufklappliste **Stationstyp** den Typ des analogen Endgeräts (z. B. Fax) aus.

d) Wählen Sie im Bereich **Durchwahl für Internet-Telefonie** aus einer Aufklappliste eine Durchwahlnummer aus. Für jeden aktiven ITSP wird Ihnen eine Aufklappliste angezeigt.

INFO: Das Feld **Durchwahl für Internet-Telefonie** ist nicht sichtbar, wenn die Internet-Telefonie nicht eingerichtet oder kein Internet-Telefonie-Service-Provider aktiviert ist.

---

e) Weisen Sie aus der Aufklappliste **Rufsignalisierung intern** dem Teilnehmer eine von insgesamt acht möglichen akustischen Rufsignalisierungen für interne Anrufe zu. Dadurch sendet der Teilnehmer anderen internen Teilnehmern einen veränderten Rufton, durch den er von anderen Teilnehmern unterschieden werden kann (Standard: Rufart 1).

f) Weisen Sie aus der Aufklappliste **Rufsignalisierung extern** dem Teilnehmer eine von insgesamt drei möglichen akustischen Rufsignalisierungen für externe Anrufe zu (Standard: Rufart 1).

g) Klicken Sie auf **OK & Weiter**.

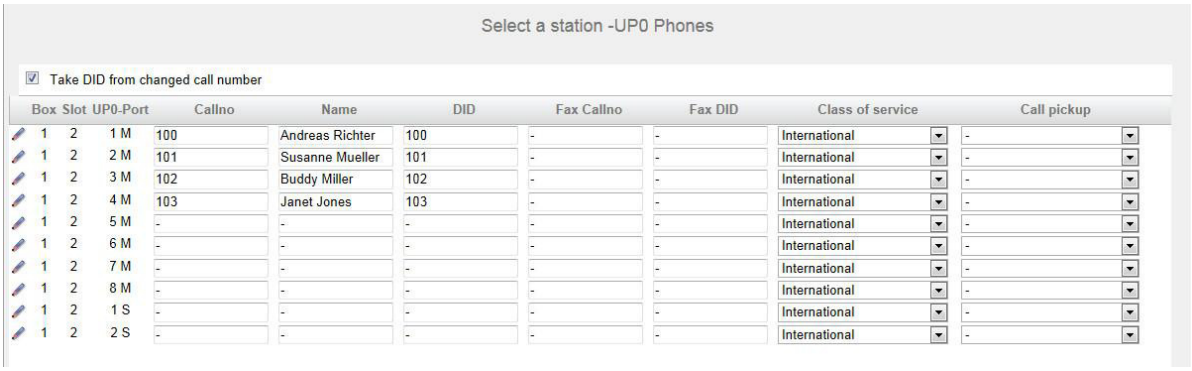
8) Wenn Sie einen weiteren analogen Teilnehmer einrichten möchten, klicken Sie auf **Daten speichern** und wiederholen Sie die Schritte 1 bis 7.

9) Klicken Sie auf **OK & Weiter**.

4.7.7.3 Wie Sie UP0-Teilnehmer konfigurieren

Voraussetzungen

- Sie befinden sich im Fenster **Teilnehmer auswählen - UP0-Endgeräte**.
- Ein Mainboard oder eine Baugruppe mit UP0-Schnittstellen ist vorhanden.



Schritt für Schritt

1) Wenn sich die Durchwahlnummer des Teilnehmers von seiner Rufnummer unterscheiden soll, geben Sie in der Zeile des gewünschten Teilnehmers unter **DuWa** eine Durchwahl-Nummer für den Teilnehmer ein:

- nur bei Anlagenanschluss:

  Klicken Sie in das gewünschte Feld und geben Sie über die Tastatur die Durchwahlnummer ein. Die Durchwahlnummer kann auch mit der internen Rufnummer identisch sein.

- nur bei Mehrgeräteanschluss:

  Wählen Sie in dem gewünschten Feld über die Aufklappliste eine MSN aus. Der Teilnehmer kann z. B. von intern über die interne Rufnummer 101 und von extern über die MSN 654321 erreicht werden.

- bei Anlagenanschluss und Mehrgeräteanschluss:

  Wählen Sie in dem gewünschten Feld über die Aufklappliste den Eintrag **xxx - änderbar** aus (xxx steht für die interne Rufnummer) und geben Sie über die Tastatur die Durchwahlnummer ein oder wählen Sie über die Aufklappliste eine MSN aus.

2) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Rufnr** eine interne Rufnummer für den Teilnehmer ein. Sie können die vorbelegte Rufnummer verwenden oder eine andere, noch nicht belegte Rufnummer vergeben.

3) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Name** einen Namen in der Form `Nachname, Vorname` oder `Vorname Nachname` ein.

INFO: Der Name kann aus bis zu 16 Zeichen bestehen, darf aber keine Umlaute oder Sonderzeichen enthalten.

4) Wenn für den Teilnehmer eine Faxbox eingerichtet werden soll (nutzbar z. B. mit den UC Clients **myPortal for Desktop** oder **myPortal for Outlook**), gehen Sie folgendermaßen vor:

a) Geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax Rufnr** die gewünschte interne Fax-Rufnummer ein, unter der der Teilnehmer von intern Faxnachrichten empfangen kann.

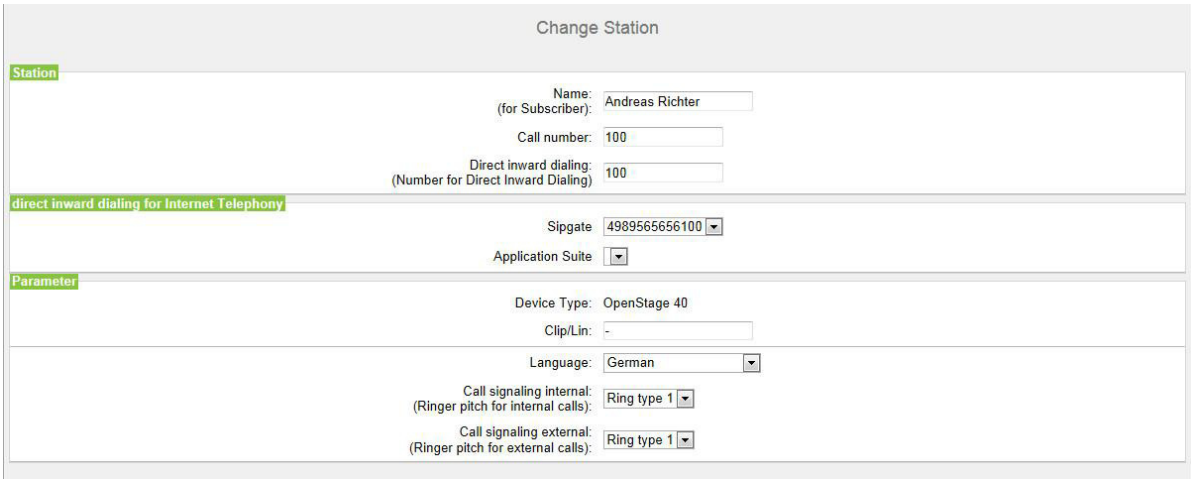
b) Wenn für die Faxbox eine Durchwahlnummer konfiguriert werden soll, geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax Durchwahl** die gewünschte externe Fax-Rufnummer ein, unter der der Teilnehmer von extern Faxnachrichten empfangen kann.

5) Wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Berechtigung** die gewünschte Berechtigungsgruppe aus.

6) Um den Teilnehmer in eine Anrufübernahmegruppe aufzunehmen, wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Anrufübernahme** eine Anrufübernahmegruppe aus.

7) Führen Sie die unter diesem Schritt beschriebenen Einstellungen nur bei Bedarf durch:

a) Klicken Sie in der Zeile des gewünschten Teilnehmers auf das Stiftsymbol **Bearbeiten**.



b) Geben Sie im Feld **Clip/Lin** eine Rufnummer ein (Durchwahlnummer oder MSN), die beim einem externen Anruf im Display des Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird.

INFO: Dieses Leistungsmerkmal muss vom Netzanbieter freigegeben sein.

c) Wählen Sie aus der Aufklappliste **Stationstyp** den Typ des TDM-Endgeräts aus.

d) Belassen Sie die Standard-Auswahl in der Aufklappliste **Sprache**. Für TDM-Endgeräte ist diese Einstellung ohne Bedeutung.

e) Wählen Sie im Bereich **Durchwahl für Internet-Telefonie** aus einer Aufklappliste eine Durchwahlnummer aus. Für jeden aktiven ITSP wird Ihnen eine Aufklappliste angezeigt.

INFO: Das Feld **Durchwahl für Internet-Telefonie** ist nicht sichtbar, wenn die Internet-Telefonie nicht eingerichtet oder kein Internet-Telefonie-Service-Provider aktiviert ist.

---

f) Weisen Sie aus der Aufklappliste **Rufsignalisierung intern** dem Teilnehmer eine von insgesamt acht möglichen akustischen Rufsignalisierungen für interne Anrufe zu. Dadurch sendet der Teilnehmer anderen internen Teilnehmern einen veränderten Rufton, durch den er von anderen Teilnehmern unterschieden werden kann (Standard: Rufart 1).

g) Weisen Sie aus der Aufklappliste **Rufsignalisierung extern** dem Teilnehmer eine von insgesamt drei möglichen akustischen Rufsignalisierungen für externe Anrufe zu (Standard: Rufart 1).

h) Klicken Sie auf **OK & Weiter**.

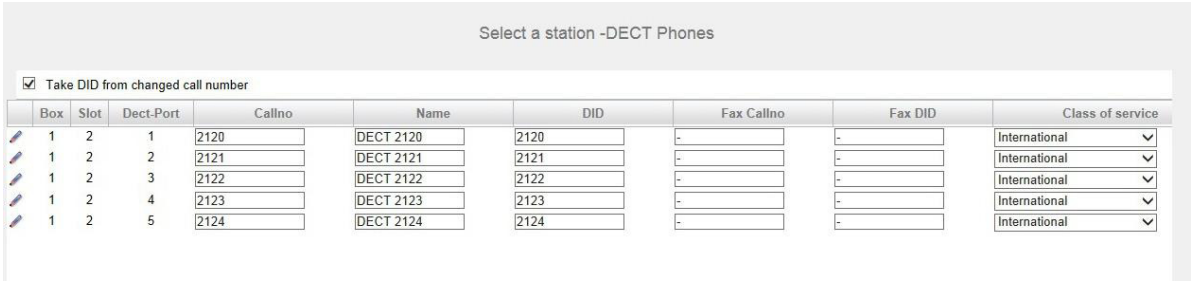
8) Wenn Sie einen weiteren UP0-Teilnehmer einrichten möchten, klicken Sie auf **Daten speichern** und wiederholen Sie die Schritte 1 bis 7.

9) Klicken Sie auf **OK & Weiter**.

4.7.7.4 Wie Sie DECT-Teilnehmer konfigurieren

Voraussetzungen

- Sie befinden sich im Fenster **Teilnehmer auswählen - DECT-Endgeräte**.
- Für die Konfiguration von DECT-Teilnehmern muss eine Basisstation angeschlossen und die DECT-Telefone dort angemeldet sein. Ist dies nicht der Fall, überspringen Sie dieses Fenster. Sie können die DECT-Teilnehmer auch später noch konfigurieren (siehe *Konfiguration der Teilnehmer*).



Schritt für Schritt

1) Wenn sich die Durchwahlnummer des Teilnehmers von seiner Rufnummer unterscheiden soll, geben Sie in der Zeile des gewünschten Teilnehmers unter **DuWa** eine Durchwahl-Nummer für den Teilnehmer ein:

- nur bei Anlagenanschluss:

  Klicken Sie in das gewünschte Feld und geben Sie über die Tastatur die Durchwahlnummer ein. Die Durchwahlnummer kann auch mit der internen Rufnummer identisch sein.

- nur bei Mehrgeräteanschluss:

  Wählen Sie in dem gewünschten Feld über die Aufklappliste eine MSN aus. Der Teilnehmer kann z. B. von intern über die interne Rufnummer 101 und von extern über die MSN 654321 erreicht werden.

- bei Anlagenanschluss und Mehrgeräteanschluss:

  Wählen Sie in dem gewünschten Feld über die Aufklappliste den Eintrag **xxx - änderbar** aus (xxx steht für die interne Rufnummer) und geben Sie über die Tastatur die Durchwahlnummer ein oder wählen Sie über die Aufklappliste eine MSN aus.

2) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Rufnr** eine interne Rufnummer für den Teilnehmer ein. Sie können die vorbelegte Rufnummer verwenden oder eine andere, noch nicht belegte Rufnummer vergeben.

3) Wenn für den Teilnehmer eine Faxbox eingerichtet werden soll (nutzbar z. B. mit den UC Clients **myPortal for Desktop** oder **myPortal for Outlook**), gehen Sie folgendermaßen vor:

a) Geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax Rufnr** die gewünschte interne Fax-Rufnummer ein, unter der der Teilnehmer von intern Faxnachrichten empfangen kann.

b) Wenn für die Faxbox eine Durchwahlnummer konfiguriert werden soll, geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax Durchwahl** die gewünschte externe Fax-Rufnummer ein, unter der der Teilnehmer von extern Faxnachrichten empfangen kann.

4) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Name** einen Namen in der Form `Nachname, Vorname` oder `Vorname Nachname` ein.

INFO: Der Name kann aus bis zu 16 Zeichen bestehen, darf aber keine Umlaute oder Sonderzeichen enthalten.

---

5) Wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Berechtigung** die gewünschte Berechtigungsgruppe aus.

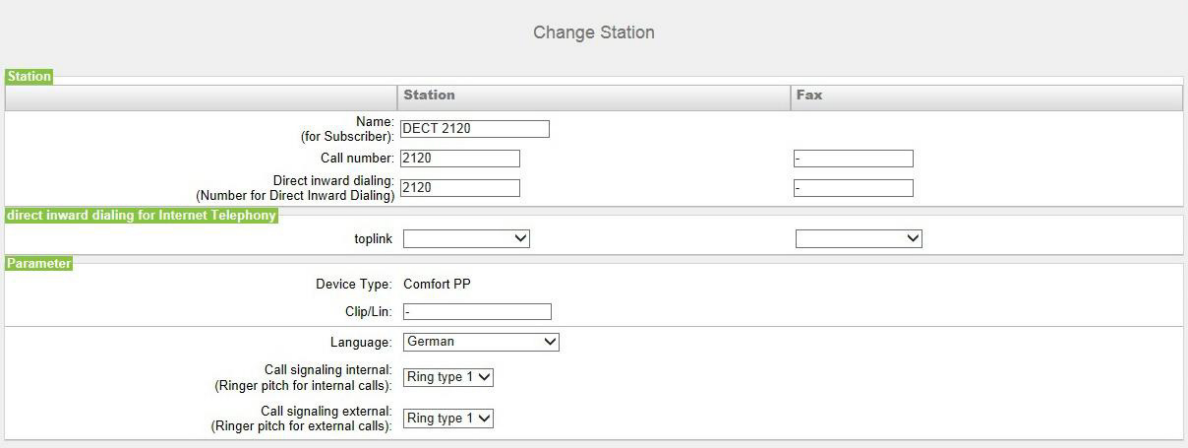
6) Um den Teilnehmer in eine Anrufübernahmegruppe aufzunehmen, wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Anrufübernahme** eine Anrufübernahmegruppe aus.

7) Falls Sie den DECT-Telefoncode (PIN) ändern wollen, geben Sie in der Zeile des gewünschten Teilnehmers unter **Mobilcode** den neuen Code ein. Der

DECT-Teilnehmer muss sich mit diesem Code neu an der Basisstation anmelden.

8) Führen Sie die unter diesem Schritt beschriebenen Einstellungen nur bei Bedarf durch:

a) Klicken Sie in der Zeile des gewünschten Teilnehmers auf das Stiftsymbol **Bearbeiten**.



b) Geben Sie im Feld **Clip/Lin** eine Rufnummer ein (Durchwahlnummer oder MSN), die beim einem externen Anruf im Display des Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird.

INFO: Dieses Leistungsmerkmal muss vom Netzanbieter freigegeben sein.

---

c) Wählen Sie aus der Aufklappliste **Stationstyp** den Typ des Schnurlos-Endgeräts aus.

d) Belassen Sie die Standard-Auswahl in der Aufklappliste **Sprache**. Für Schnurlos-Endgeräte ist diese Einstellung ohne Bedeutung.

e) Wählen Sie im Bereich **Durchwahl für Internet-Telefonie** aus einer Aufklappliste eine Durchwahlnummer aus. Für jeden aktiven ITSP wird Ihnen eine Aufklappliste angezeigt.

INFO: Das Feld **Durchwahl für Internet-Telefonie** ist nicht sichtbar, wenn die Internet-Telefonie nicht eingerichtet oder kein Internet-Telefonie-Service-Provider aktiviert ist.

---

f) Weisen Sie aus der Aufklappliste **Rufsignalisierung intern** dem Teilnehmer eine von insgesamt acht möglichen akustischen Rufsignalisierungen für interne Anrufe zu. Dadurch sendet der Teilnehmer anderen internen Teilnehmern einen veränderten Rufton, durch den er von anderen Teilnehmern unterschieden werden kann (Standard: Rufart 1).

g) Weisen Sie aus der Aufklappliste **Rufsignalisierung extern** dem Teilnehmer eine von insgesamt drei möglichen akustischen Rufsignalisierungen für externe Anrufe zu (Standard: Rufart 1).

h) Klicken Sie auf **OK & Weiter**.

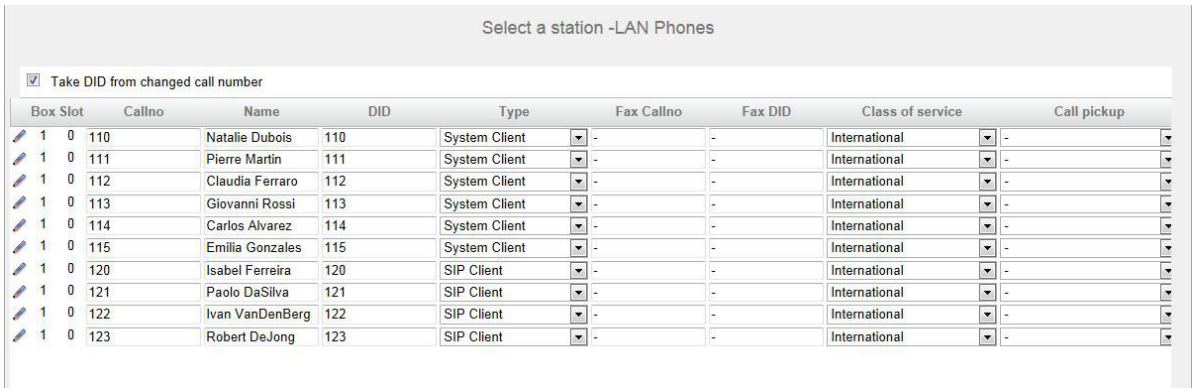
9) Wenn Sie einen weiteren Teilnehmer einrichten möchten, klicken Sie auf **Daten speichern** und wiederholen Sie die Schritte 1 bis 8.

10) Klicken Sie auf **OK & Weiter**.

4.7.7.5 Wie Sie IP- und SIP-Teilnehmer konfigurieren

Voraussetzungen

- Sie befinden sich im Fenster **Teilnehmer auswählen - LAN-Telefone**.
- Für den Betrieb von WLAN-Telefonen benötigen Sie ein funktionsfähiges Wireless-LAN-Netzwerk.



Schritt für Schritt

1) Wenn sich die Durchwahlnummer des Teilnehmers von seiner Rufnummer unterscheiden soll, geben Sie in der Zeile des gewünschten Teilnehmers unter **DuWa** eine Durchwahl-Nummer für den Teilnehmer ein:

- nur bei Anlagenanschluss:

  Klicken Sie in das gewünschte Feld und geben Sie über die Tastatur die Durchwahlnummer ein. Die Durchwahlnummer kann auch mit der internen Rufnummer identisch sein.

- nur bei Mehrgeräteanschluss:

  Wählen Sie in dem gewünschten Feld über die Aufklappliste eine MSN aus. Der Teilnehmer kann z. B. von intern über die interne Rufnummer 101 und von extern über die MSN 654321 erreicht werden.

- bei Anlagenanschluss und Mehrgeräteanschluss:

  Wählen Sie in dem gewünschten Feld über die Aufklappliste den Eintrag **xxx - änderbar** aus (xxx steht für die interne Rufnummer) und geben Sie über die Tastatur die Durchwahlnummer ein oder wählen Sie über die Aufklappliste eine MSN aus.

2) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Rufnr** eine interne Rufnummer für den Teilnehmer ein. Sie können die vorbelegte

Rufnummer verwenden oder eine andere, noch nicht belegte Rufnummer vergeben.

3) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Name** einen Namen in der Form `Nachname, Vorname` ein.

> ***INFO:*** Der Name kann aus bis zu 16 Zeichen bestehen, sollte aber keine Umlaute oder Sonderzeichen enthalten. Der Name wird wie hier angegeben bei den UC Clients als Nachname eingetragen, kann dort aber nachbearbeitet werden.

4) Wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Typ** den Typ des IP-Teilnehmers aus (z. B. "System Client" oder "SIP Client").

5) Wenn für den Teilnehmer eine Faxbox eingerichtet werden soll (nutzbar z. B. mit den UC Clients **myPortal for Desktop** oder **myPortal for Outlook**), gehen Sie folgendermaßen vor:

a) Geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax Rufnr** die gewünschte interne Fax-Rufnummer ein, unter der der Teilnehmer von intern Faxnachrichten empfangen kann.

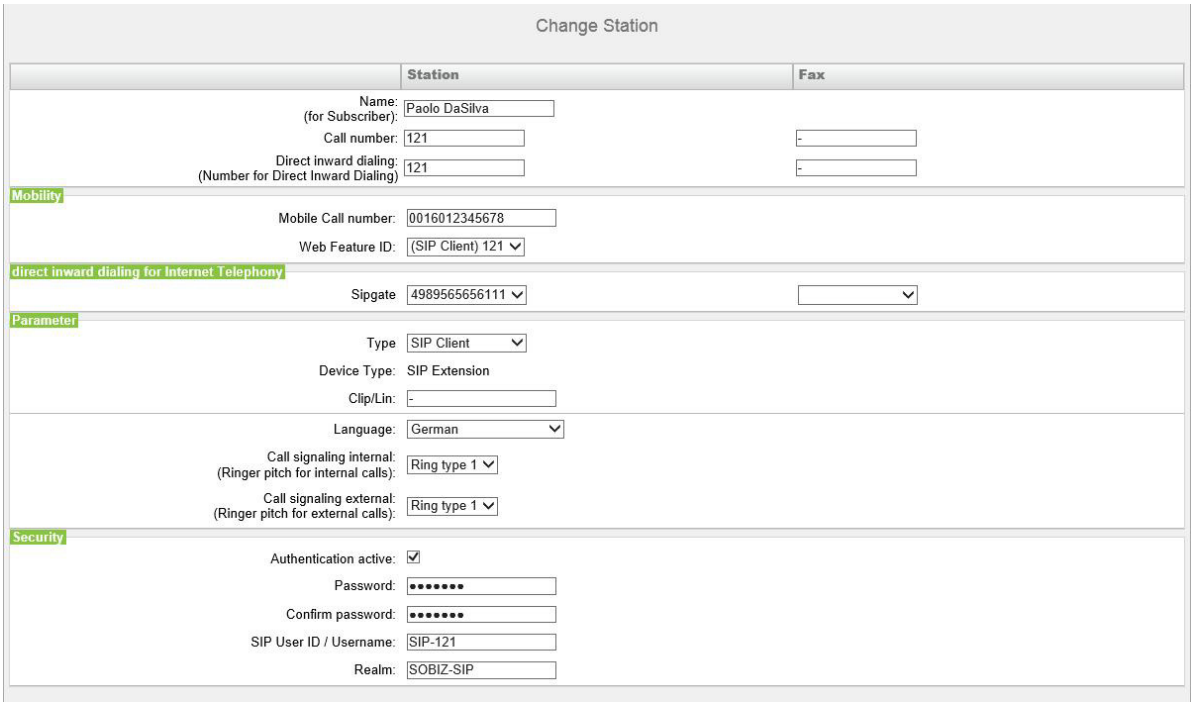
b) Wenn für die Faxbox eine Durchwahlnummer konfiguriert werden soll, geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax Durchwahl** die gewünschte externe Fax-Rufnummer ein, unter der der Teilnehmer von extern Faxnachrichten empfangen kann.

6) Wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Berechtigung** die gewünschte Berechtigungsgruppe aus.

7) Um den Teilnehmer in eine Anrufübernahmegruppe aufzunehmen, wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Anrufübernahme** eine Anrufübernahmegruppe aus.

8) Führen Sie die unter diesem Schritt beschriebenen Einstellungen nur bei Bedarf oder für ein SIP-Telefon durch:

a) Klicken Sie in der Zeile des gewünschten Teilnehmers auf das Stiftsymbol **Bearbeiten**.



b) Nur für SIP-Telefone: Wenn das SIP-Telefon zusammen mit einem Dual-Mode-Mobiltelefon betrieben werden soll, geben Sie im Bereich Mobility unter mobile Rufnummer die Amtskennziffer gefolgt von der Rufnummer des Mobiltelefons ein (z. B. 0016012345678). Wählen Sie zusätzlich aus der Aufklappliste Web Feature ID diesen SIP Client aus. (siehe *Dual-Mode-Telefonie*).

c) Geben Sie im Feld **Clip/Lin** eine Rufnummer ein (Durchwahlnummer oder MSN), die beim einem externen Anruf im Display des Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird.

INFO: Dieses Leistungsmerkmal muss vom Netzanbieter freigegeben sein.

---

d) Wählen Sie aus der Aufklappliste **Sprache** die Sprache für die Menüsteuerung des Telefons aus.

e) Weisen Sie aus der Aufklappliste **Rufsignalisierung intern** dem Teilnehmer eine von insgesamt acht möglichen akustischen Rufsignalisierungen für interne Anrufe zu. Dadurch sendet der Teilnehmer anderen internen Teilnehmern einen veränderten Rufton, durch den er von anderen Teilnehmern unterschieden werden kann (Standard: Rufart 1).

f) Weisen Sie aus der Aufklappliste **Rufsignalisierung extern** dem Teilnehmer eine von insgesamt drei möglichen akustischen Rufsignalisierungen für externe Anrufe zu (Standard: Rufart 1).

g) Nur für SIP-Telefone: Aktiveren Sie das Kontrollkästchen **Authentifizierung aktiv**.

h) Nur für SIP-Telefone: Geben Sie in den Feldern **Kennwort** und **Kennwort bestätigen** das Kennwort für die Authentifizierung ein.

i) Nur für SIP-Telefone: Geben Sie im Feld **SIP User ID / Benutzername** die Benutzerkennung für die Authentifizierung ein.

j) Nur für SIP-Telefone: Geben Sie im Feld **Realm** die zugehörige Zone für die Authentifizierung ein.

k) Klicken Sie auf **OK & Weiter**.

9) Wenn Sie einen weiteren IP-Teilnehmer einrichten möchten, klicken Sie auf **Daten speichern** und wiederholen Sie die Schritte 1 bis 8.

10) Klicken Sie auf **OK & Weiter**. Sie sehen eine Liste aller eingerichteten Teilnehmer. Diese Liste entspricht einem Rufnummernplan.

11) Klicken Sie bei Bedarf auf **Drucken**, um die Daten der eingerichteten Teilnehmer auszudrucken.

12) Klicken Sie anschließend auf **OK & Weiter**.

4.7.8 Konfiguration von UC Suite (nur mit UC Booster Card)

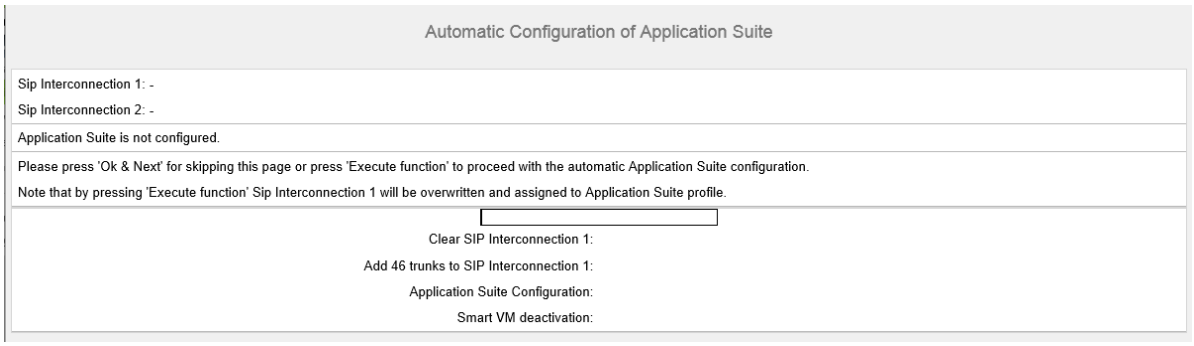
Im Fenster **Automatische Konfiguration der Applikation-Suite** können Sie die automatische Konfiguration der UC-Lösung UC Suite durchführen.

INFO: Dieses Fenster erscheint nur, wenn eine UC Booster Card im Kommunikationssystem montiert ist.

4.7.8.1 Wie Sie UC Suite konfigurieren

Voraussetzungen

- Sie befinden sich im Fenster **Automatische Konfiguration der Application Suite**.



Schritt für Schritt

1) Wenn keine UC Booster Card in das Kommunikationssystem integriert ist, klicken Sie auf **OK & Weiter**. Die Konfiguration wird übersprungen.
2) Wenn die UC Booster Card in das Kommunikationssystem integriert ist, klicken Sie auf **Funktion ausführen**. Die UC Suite wird automatisch konfiguriert. Sobald der Verlaufsbalken 100% anzeigt, klicken Sie auf **OK & Weiter**.

4.7.9 Konfiguration der UC Smart Sprachboxen (nur mit UC Smart)

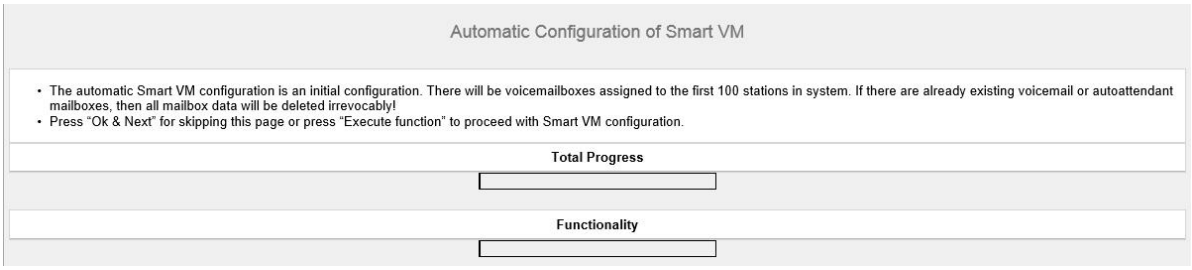
Im Fenster **Automatische Konfiguration der Smart VM** können Sie die automatische Konfiguration der UC Smart Sprachboxen (Smart VM, Smart VoiceMail) durchführen, wenn die UC-Lösung UC Smart genutzt wird.

INFO: Dieses Fenster erscheint nur, wenn im Wizard **Erstinstallation** bei der Applikationsauswahl **Paket mit UC Smart** gewählt wurde.

4.7.9.1 Wie Sie die UC Smart Sprachboxen konfigurieren

Voraussetzungen

- Sie befinden sich im Fenster **Automatische Konfiguration der Smart VM**.



Schritt für Schritt

1) Wenn die UC Smart Sprachboxen nicht genutzt werden sollen, klicken Sie auf **OK & Weiter**. Die Konfiguration der Sprachboxen wird übersprungen.
2) Wenn die UC Smart Sprachboxen genutzt werden sollen, klicken Sie auf **Funktion ausführen**. Für die ersten 100 Teilnehmer werden automatisch Sprachboxen konfiguriert. Sobald der Verlaufsbalken 100% anzeigt, klicken Sie auf **OK & Weiter**.

INFO: Bereits vorhandene UC Smart Sprachboxen oder UC Smart AutoAttendant-Sprachboxen werden dabei unwiderruflich gelöscht.

4.7.10 Konferenz-Server-Einstellungen (nur mit UC Suite)

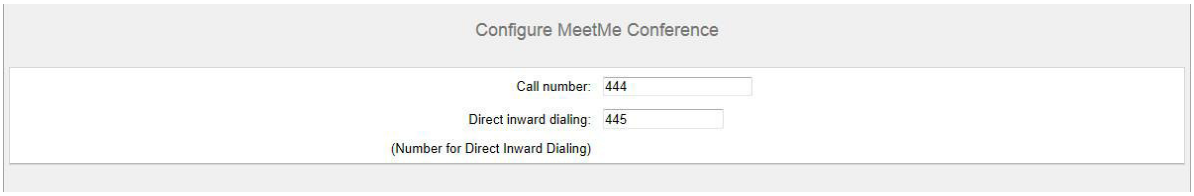
Im Fenster **MeetMe-Konferenz-Einstellungen ändern** können Sie die Rufnummer und die Einwahlnummer für Konferenzen festlegen.

INFO: Dieses Fenster erscheint nur, wenn im Wizard **Erstinstallation** bei der Applikationsauswahl **Paket mit UC Suite ...** gewählt wurde.

4.7.10.1 Wie Sie die Konferenz-Server-Einstellungen ändern

Voraussetzungen

- Die Hard- und Software für die Nutzung von UC Suite ist vorhanden.
- Sie befinden sich im Fenster **MeetMe-Konferenz-Einstellungen ändern**.



Schritt für Schritt

1) Geben Sie im Feld **Rufnummer** eine Rufnummer für die Konferenz ein.

2) Legen Sie im Feld **Durchwahl** die Einwahlnummer für die Konferenz (Konferenz-DUWA) fest, mit der sich Teilnehmer in eine bestehende Konferenz einwählen können.

3) Klicken Sie auf **OK & Weiter**.

4.7.11 E-Mail-Versand (optional)

Im Fenster **E-Mail-Weiterleitung ändern** können Sie den E-Mail-Versand konfigurieren. Teilnehmer werden dadurch über neue Sprach- und Faxnachrichten informiert und der Administrator erhält Systemmeldungen.

Sie haben folgende Möglichkeiten:

- E-Mail-Versand konfigurieren
  Sie können einen externen E-Mail-Server festlegen, über den OpenScape Business die E-Mails versenden soll. Sprach- und Faxnachrichten oder interne Systemmeldungen werden über diesen E-Mail-Server an eine oder verschiedene konfigurierbare E-Mail-Adressen versendet.

INFO: Die Angabe eines E-Mail-Servers ist wichtig, wenn den Benutzern der UC Suite automatisch per E-Mail ein Link auf die Installationsdatei(en) geschickt werden soll.

4.7.11.1 Wie Sie den E-Mail-Versand konfigurieren

Voraussetzungen

- Es ist ein E-Mail-Konto mit einem Kennwort bei einem E-Mail-Provider vorhanden und Sie kennen die Zugangsdaten.
- Sie befinden Sich im Fenster **E-Mail-Weiterleitung ändern**.



Schritt für Schritt

1) Geben Sie den **Postausgangs-Server (SMTP)** für den E-Mail-Server ein, der für den E-Mail-Versand genutzt werden soll, z. B. `smtp.web.de`. Erfragen Sie den Postausgangs-Server ggf. bei Ihrem E-Mail-Provider.

INFO: Achten Sie darauf, dass der Name des Postausgangs-Servers aufgelöst werden kann. Falls nicht, müssen Sie den Wizard für den E-Mail-Versand starten über **Service-Center > Email-Weiterleitung** und anstelle des Namens des Postausgangs-Servers die IP-Adresse des Postausgangs-Servers eingeben.

2) Wenn eine sichere Verbindung erforderlich ist, aktivieren Sie das Kontrollkästchen. Erfragen Sie ggf. bei Ihrem E-Mail-Provider, ob diese Option aktiviert werden muss.

3) Geben Sie den **Benutzernamen** des E-Mail-Kontos ein z. B. `max.mustermann`.

4) Geben Sie unter **Kennwort** und **Kennwort wiederholen** das Kennwort des E-Mail-Kontos ein.

5) Geben Sie die **E-Mail-Adresse** ein, z. B. `max.mustermann@web.de`.

6) Wenn Sie die eingegebenen E-Mail-Einstellungen sofort testen wollen, gehen Sie folgendermaßen vor:

a) Klicken Sie auf **Weiterleitung testen**.

b) Geben Sie unter **Senden an E-Mail-Adresse** die E-Mail-Adresse eines E-Mail-Postfachs ein, auf das Sie Zugriff haben. An diese E-Mail-Adresse wird die Test-E-Mail geschickt.

c) Geben Sie unter **Betreff in der Email** einen beschreibenden Text ein, um die E-Mail in Ihrem E-Mail-Postfach identifizieren zu können.

d) Klicken Sie auf **Testmail senden**. Die E-Mail-Einstellungen werden überprüft und die E-Mail an das angegebene E-Mail-Postfach abgeschickt.

e) Überprüfen Sie, ob die E-Mail in Ihrem E-Mail-Postfach angekommen ist.

f) War der E-Mail-Versand erfolgreich, gehen Sie zum nächsten Schritt.

g) War der E-Mail-Versand nicht erfolgreich, klicken Sie auf **Zurück** und überprüfen nochmal Ihre E-Mail-Einstellungen.

7) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**. Die Basisinstallation ist beendet. Bevor Sie die im Wizard erwähnte Datensicherung durchführen, sollten Sie die Lizenzen aktivieren.

4.8 Abschließende Tätigkeiten

Nachdem die Erstinstallation und die Basisinstallation mit dem WBM abgeschlossen sind, müssen noch einige wichtige Einstellungen für den Betrieb von OpenScape Business getroffen werden.

Gehen Sie folgendermaßen vor:

1. Remote Service SSDP einschalten
   Sie können den autorisierten Servicetechnikern eines Remote Service Partners den Fernzugriff auf das Kommunikationssystem ermöglichen. Damit ist z. B. die Unterstützung bei der Lösung von Administrationsaufgaben oder bei der Fehlersuche möglich.
   Die Variante mit höchster Sicherheit ist der Fernzugriff über die internetbasierte Plattform für Remote Services SSDP (Smart Services Delivery Platform). Jeder Remote Service Partner, der SSDP nutzt, hat eine eigene Partner ID. Mit der vorbelegten Partner ID "Unify" kann der Fernzugriff durch autorisiertes Servicepersonal des Herstellers aktiviert werden.
   Für die Konfiguration von SSDP und für weitere Varianten einen Remote-Zugang einzurichten siehe *Remote Services*
2. Lizenzen aktivieren und zuordnen
   Die mit OpenScape Business erworbenen Lizenzen müssen innerhalb einer Zeitspanne von 30 Tagen aktiviert werden. Die Zeitspanne startet beim ersten Anmelden am WBM. Nach Ablauf der Zeitspanne ist das Kommunikationssystem nur noch eingeschränkt nutzbar. Nach erfolgreicher Aktivierung müssen die Lizenzen den Teilnehmern und Leitungen zugeordnet werden.

Systemweite Leistungsmerkmale sind in einem Standalone-System bereits mit der Aktivierung freigeschaltet.

3. UC Clients zur Installation bereitstellen (nur für UC Suite)
   Die UC Clients sind Bestandteil der UC Suite. Die Installationsdateien für die UC Clients sind über das WBM zugänglich und können den IP-Teilnehmern automatisch oder manuell zur Verfügung gestellt werden.
   Zusätzlich gibt es für den Administrator die Möglichkeit der Silent Installation. Dabei handelt es sich um eine kommandozeilenbasierte Methode zur automatischen Installation, Deinstallation und Modifikation von UC Suite Clients auf einem PC ohne weitere erforderliche Eingaben. Für weitere Informationen siehe *Silent Installation/Deinstallation für UC Suite PC-Clients*.
4. Datensicherung durchführen
   Die bisherigen Änderungen an OpenScape Business müssen gesichert werden. Die Sicherung kann als Backup-Set z. B. auf einem USB-Medium oder im internen Netz gespeichert werden.

4.8.1 Wie Sie den Remote Service SSDP einschalten

Voraussetzungen

- Ein Internet-Zugang und eine funktionierende DNS-Konfiguration liegen vor.
- Die Partner ID Ihres Remote Service Partners liegt vor (vorbelegte Partner ID: Unify)
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Remote-Zugang**.

3) Klicken Sie auf **Aktivierung / Deaktivierung**, um den Wizard **Aktivierung / Deaktivierung des Service-Plugin** zu starten.

4) Ändern Sie im Feld **Partner ID** bei Bedarf die vorbelegte Partner ID und klicken Sie auf **Sichern**.

5) Klicken Sie auf **Aktivieren**.

4.8.2 Wie Sie die Lizenzen aktivieren und zuordnen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.
- Sie kennen den LAC (Lizenz-Autorisierungscode) für die Lizenzfreischaltung und haben eine Benutzerkennung und ein Passwort für den Zugang zum Lizenzserver.
- Für die Verbindung zum Lizenzserver ist ein Internet-Zugang nötig.

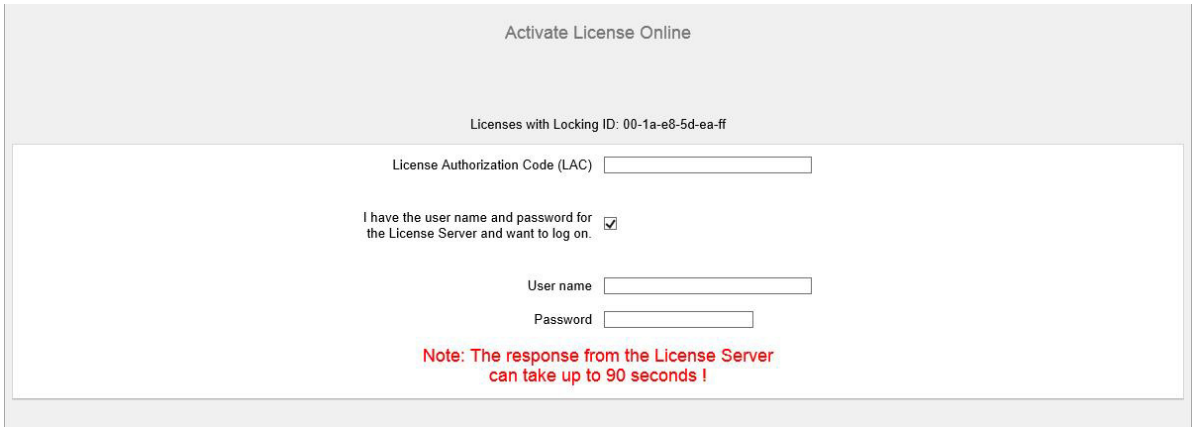
Schritt für Schritt

1) Lizenzen online aktivieren:

a) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

b) Klicken Sie im Navigationsbaum auf **Wizards > Grundinstallation**.

c) Klicken Sie auf **Bearbeiten**, um den Wizard **Lizenzierung** zu starten.



d) Geben Sie im Feld **Lizenz Autorisierungs Code (LAC)** den LAC ein.

e) Aktivieren Sie das Kontrollkästchen **Ich habe Benutzernamen und Kennwort für den Lizenzserver und möchte mich anmelden**.

f) Geben Sie **Benutzername** und **Kennwort** für die Anmeldung am Lizenzserver ein.

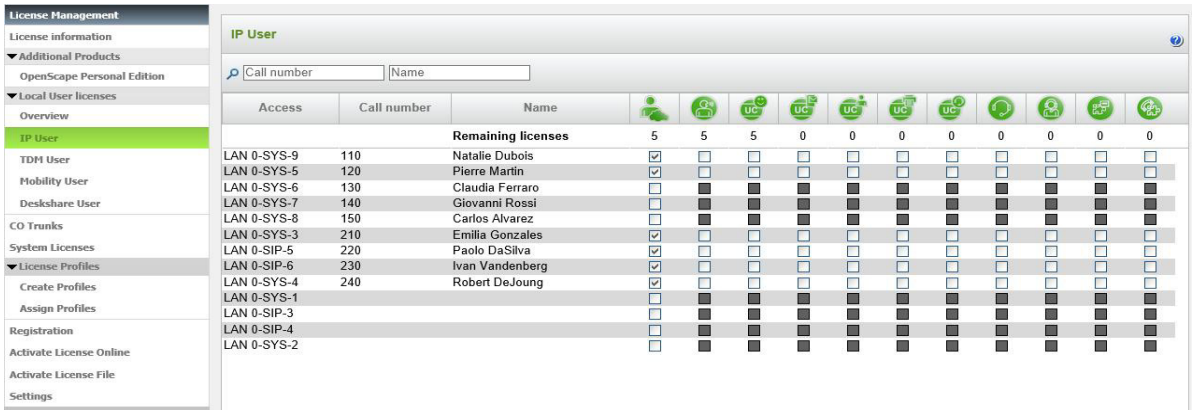
g) Klicken Sie auf **OK & Weiter**. Die Verbindung zum Lizenzserver wird hergestellt und die Lizenzen freigeschaltet.

2) Lizenzen den Teilnehmern zuordnen:

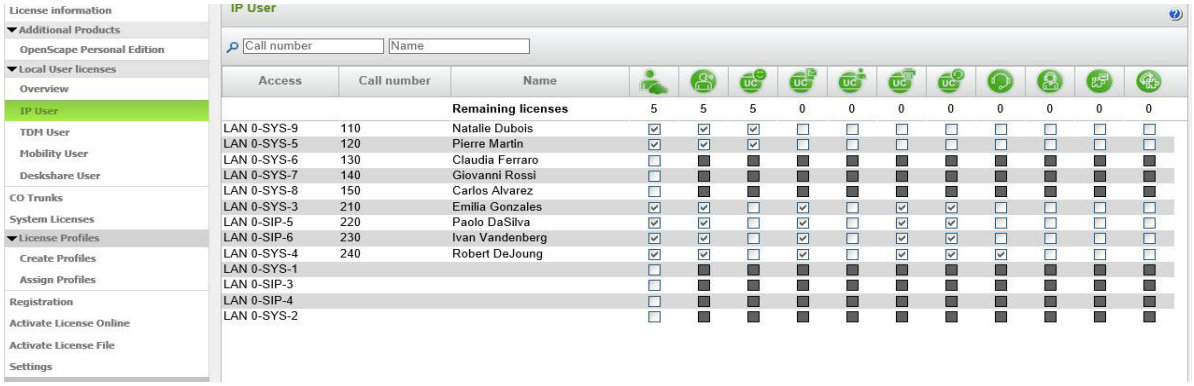
a) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.

b) Navigieren Sie im Navigationsbaum auf **Lokale Benutzerlizenzen > ...** zum gewünschten Teilnehmer-Typ. Es wird Ihnen eine Liste aller Teilnehmer des ausgewählten Teilnehmer-Typs angezeigt.

c) Aktivieren Sie in der Zeile des gewünschten Teilnehmers das Kontrollkästchen in der Spalte **Benutzer-Lizenz** (erste Spalte mit Kontrollkästchen).



d) Aktivieren Sie in der Zeile des gewünschten Teilnehmers die User-orientierten Lizenzen, indem Sie die gewünschten Kontrollkästchen aktivieren.



INFO: User-orientierte Lizenzen können einem Teilnehmer nur zugewiesen werden, wenn dem Teilnehmer zuvor eine Teilnehmer-Lizenz (Benutzer-Lizenz) zugeordnet wurde (Schritt c).

---

e) Klicken Sie auf **OK & Weiter**. Es wird geprüft, ob für Ihre Zuordnung genügend Lizenzen vorhanden sind.

Sind ausreichend Lizenzen vorhanden ist die Lizenzierung der Teilnehmer beendet.

f) Fehlen Lizenzen, werden Ihnen die Fehler mit einem rot hinterlegten Kontrollkästchen angezeigt. Korrigieren Sie diese Fehler und wiederholen Sie Schritt e.

3) Lizenzen den Leitungen zuordnen:

a) Klicken Sie im Navigationsbaum auf **Amtsleitungen**. Im Bereich **Amtsleitungen** wird Ihnen die Anzahl der erworbenen Leitungslizenzen angezeigt.

b) Für SIP-Leitungen: Geben Sie im Bereich **Bedarf an Lizenzen für gleichzeitige Internet-Anrufe in diesem Knoten** die Anzahl der

Internet-Gespräche an, die gleichzeitig über einen ITSP geführt werden können.

c) Für S_{2M}-Leitungen: Wählen Sie im Bereich **S2M** in der Zeile des gewünschten Slots in der Aufklappliste der Spalte **Demands** die Anzahl der gewünschten B-Kanäle aus.

d) Für T1-Leitungen (nur USA): Wählen Sie im Bereich **T1** in der Zeile des gewünschten Slots in der Aufklappliste der Spalte **Demands** die Anzahl der gewünschten B-Kanäle aus.

e) Klicken Sie auf **OK & Weiter**.

INFO: Die Anzahl der lizenzierten SIP-Leitungen und die Anzahl der lizenzierten S_{2M}-/T1-Leitungen darf die Anzahl der erworbenen Leitungslizenzen nicht überschreiten.

4.8.3 Wie Sie die UC Suite Clients zur Installation bereitstellen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.
- Die Hard- und Software für die Nutzung von UC Suite ist vorhanden.

INFO: Für die Nutzung der UC Suite Clients sind Lizenzen nötig.

Schritt für Schritt

1) Damit die Installationsdateien einem Teilnehmer automatisch zur Verfügung gestellt werden können, vergewissern Sie sich, ob folgende Schritte durchgeführt worden sind:

a) Die E-Mail-Adressen der Teilnehmer müssen entweder zusammen mit den Teilnehmerdaten über eine XML-Datei importiert worden sein oder eingetragen werden unter **Einrichtung > UC Suite > Benutzerverzeichnis**.

b) Ein Mail-Server muss eingetragen sein.

INFO: Einen E-Mail-Server können Sie auch nachträglich eintragen unter **Service-Center > Email-Weiterleitung**.

Alle Teilnehmer, deren E-Mail-Adressen bekannt sind, erhalten eine E-Mail mit dem Link auf das Installationsverzeichnis der UC Clients und mit einer Erste-Schritte-Anleitung. Im Installationsverzeichnis liegt zusätzlich eine Readme-Datei mit Informationen zur Installation der Software auf den Client-PCs.

2) Falls die nötigen Schritte für eine automatische Benachrichtigung nicht erfüllt sind, können Sie die Installationsdateien auch manuell zur Verfügung stellen. Gehen Sie dazu folgendermaßen vor:

a) Klicken Sie in der Navigationsleiste auf **Service-Center**.

b) Klicken Sie im Navigationsbaum auf **Software**.

c) Klicken Sie auf den gewünschten UC Client und speichern Sie die gezippte Installationsdatei auf einem freigegebenen Netz-Laufwerk.

d) Klicken Sie im Navigationsbaum auf **Dokumente** und wählen Sie die Aufklappliste **Bedienungsanleitung**.

e) Klicken Sie auf die Dokumentation zum gewünschten UC Client und speichern Sie die Dokumentationsdatei auf einem freigegebenen Netz-Laufwerk.

f) Senden Sie den Benutzern der UC Clients die gezippte Installationsdatei und die Dokumentationsdatei per E-Mail oder teilen Sie den Benutzern den Ablageort der Dateien mit.

g) In der Zip-Datei mit den Installationsdateien ist auch eine Readme-Datei enthalten. Weisen Sie die Benutzer darauf hin, dass die Installation der UC Clients anhand der Installationshinweise in der Readme-Datei durchgeführt werden muss.

3) Alternativ können Sie den UC Benutzern auch Links zuschicken, über die sie direkt auf die Installationsdateien der UC Clients zugreifen können.

a) Klicken Sie in der Navigationsleiste auf **Service-Center**.

b) Klicken Sie im Navigationsbaum auf **Software**.

c) Klicken Sie auf die Schaltfläche **Applikationslinks anzeigen**. Es werden Ihnen mehrere Links angezeigt, abhängig vom verwendeten Betriebssystem und vom gewünschten UC Client, z. B.:

```
https://<IP-Adresse des Kommunikationssystems>/
management/downloads/install-common.zip
```

4.8.4 Wie Sie den UC Smart Client zur Installation bereitstellen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.
- Die Hard- und Software für die Nutzung von UC Smart ist vorhanden.

> ***INFO:*** Für die Nutzung des UC Smart Clients myPortal Smart sind Lizenzen nötig.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Software**.
3) Klicken Sie auf das Download-Symbol von **myPortal Smart** und speichern Sie die Installationsdatei auf einem freigegebenen Netz-Laufwerk.
4) Klicken Sie auf das Link-Symbol von **Adobe AIR** und laden Sie die Installationsdatei auf ein freigegebenes Netz-Laufwerk herunter.
5) Senden Sie den Benutzern des UC Clients die beiden Installationsdateien oder teilen Sie den Benutzern den Ablageort der Dateien mit.

INFO: Alternativ können Sie den UC Benutzern auch zwei Links zuschicken, über die sie auf die Installationsdateien zugreifen können:

`https://<IP-Adresse des Kommunikationssystems>/management/downloads/SmartClient.air`

`http://www.adobe.com/air`

4.8.5 Wie Sie die Datensicherung durchführen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.
- Für eine Datensicherung auf einem USB-Medium (USB-Stick oder USB-Festplatte) muss das USB-Medium an der USB-Server-Schnittstelle angeschlossen sein.

INFO: Weitere Informationen zur Datensicherung siehe *Sofortiges Sichern*.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Datensicherung**.
2) Klicken Sie im Navigationsbaum auf **Backup - sofort**.
3) Geben Sie im Bereich **Name** im Feld **Kommentar** einen Kommentar für das Backup-Set ein, um das Backup-Set bei einer möglichen Wiederherstellung leichter identifizieren zu können. Vermeiden Sie bei der Eingabe Umlaute und Sonderzeichen.
4) Aktivieren Sie im Bereich **Geräte** das Ziellaufwerk, auf dem das Backup-Set gespeichert werden soll.
5) Klicken Sie auf **OK & Weiter**. In einem weiteren Fenster wird Ihnen der Fortschritt der Sicherung angezeigt.

6) Die Sicherung ist erfolgreich, wenn die Meldung **Sicherung erfolgreich ausgeführt!** erscheint. Klicken Sie auf **Beenden**.

7) Wenn Sie als Backup-Medium einen USB-Stick verwenden, warten Sie ab, bis die LED des USB-Sticks aufhört zu blinken. Erst dann ist die Sicherung erfolgreich auf dem USB-Stick gespeichert. Entfernen Sie anschließend den USB-Stick.

8) Die Erstinbetriebnahme mit dem WBM ist nun abgeschlossen. Beenden Sie das WBM, indem Sie rechts oben auf den Link **Abmelden** klicken und anschließend das Fenster schließen.

INFO: Falls eine neue Software-Version für das Kommunikationssystem vorliegt, wird Ihnen das auf der Startseite des WBM mitgeteilt - vorausgesetzt der Internet-Anschluss ist korrekt eingerichtet. Liegt eine neue Software-Version vor, führen Sie ein Update durch (siehe *Update des Kommunikationssystems*).

4.9 Inbetriebnahme der IP-Telefone

Eine komfortable Inbetriebnahme der IP-Telefone erfordert einen DHCP-Server, der das IP-Telefon mit den für die Anmeldung am Kommunikationssystem wichtigen Daten (netzwerkspezifische Daten) versorgt.

Netzwerkspezifische Daten

Ein IP-Telefon benötigt für die Anmeldung am Kommunikationssystem netzwerkspezifische Daten. Diese Daten können einerseits im DHCP-Server gespeichert sein oder direkt am IP-Telefon eingegeben werden. Vorteil eines DHCP-Servers ist, dass alle angeschlossenen IP-Telefone automatisch mit den Daten versorgt werden.

Folgende Daten werden vom IP-Telefon benötigt:

- IP-Adresse des Kommunikationssystems
- IP-Adresse des DLS-Servers

Zusätzlich benötigt das IP-Telefon noch die eigene Rufnummer. Diese muss während der Anmeldung manuell am Telefon eingetragen werden.

Registrierung von SIP-Telefonen

Aus Sicherheitsgründen ist es empfehlenswert, dass sich SIP-Telefone am Kommunikationssystem registrieren. Dazu müssen die Registrationsdaten am IP-Telefon und im Kommunikationssystem übereinstimmen.

Folgende Daten werden für die Anmeldung benötigt:

- SIP-Benutzer-ID
- SIP-Passwort
- SIP-Realm (optional)

Verwenden Sie ein nicht triviales SIP-Passwort, das folgende Regeln erfüllt:

- Mindestens 8 Stellen
- Mindestens einen Großbuchstaben (A - Z)
- Mindestens einen Kleinbuchstaben (a - z)
- Mindestens eine Ziffer (0-9)
- Mindestens ein Sonderzeichen

Verwenden Sie eine SIP-Benutzer-ID, die nicht die Telefonnummer enthält.

INFO: Weitere Informationen zur Einrichtung von SIP-Telefonen finden Sie unter `http://wiki.unify.com/wiki/SIP_devices_configuration_examples`.

Nutzung des internen DHCP-Servers

Wird der interne DHCP-Server des Kommunikationssystems genutzt, sind die netzwerkspezifischen Daten dort bereits hinterlegt. Damit sich ein IP-Telefon am Kommunikationssystem registrieren kann, muss am IP-Telefon nur die festgelegte Rufnummer eintragen werden. Für ein SIP-Telefon müssen zusätzlich die Daten zur SIP-Registrierung am SIP-Telefon und am Kommunikationssystem übereinstimmen.

Nutzung eines externen DHCP-Servers mit netzwerkspezifischen Daten

Wird ein externer DHCP-Server genutzt, sind die netzwerkspezifischen Daten dort zu hinterlegen. Damit sich ein IP-Telefon am Kommunikationssystem registrieren kann, muss am IP-Telefon nur die festgelegte Rufnummer eintragen werden. Für ein SIP-Telefon müssen zusätzlich die Daten zur SIP-Registrierung am SIP-Telefon und am Kommunikationssystem übereinstimmen.

Nutzung eines externen DHCP-Servers ohne netzwerkspezifische Daten

Wird ein externer DHCP-Server genutzt, bei dem die netzwerkspezifischen Daten nicht hinterlegt werden können, müssen diese am IP-Telefon eingegeben werden. Damit sich ein IP-Telefon am Kommunikationssystem registrieren kann, müssen am IP-Telefon die festgelegte Rufnummer und die IP-Adresse des Kommunikationssystems eintragen und evtl. die Einstellungen für den Deployment Service geändert werden. Für ein SIP-Telefon müssen zusätzlich die Daten zur SIP-Registrierung am SIP-Telefon und am Kommunikationssystem übereinstimmen.

4.9.1 Wie Sie ein IP-Telefon konfigurieren

Voraussetzungen

- Das IP-Telefon ist an das interne Netz angeschlossen und betriebsbereit.

INFO: Hier wird die Konfiguration am Beispiel eines OpenStage 40/60/80 IP-Systemtelefons beschrieben. Für ein anderes IP-

Telefon müssen diese Einstellungen analog durchgeführt werden. Sehen Sie dazu bitte in der Anleitung Ihres IP-Telefons nach.

Schritt für Schritt

1) Um in den Administrationsmodus des IP-Systemtelefons zu gelangen, drücken Sie am Telefon die Taste für das Einstellungen-/Anwendungen-Menü.

2) Blättern Sie im Register `Einstellungen` bis `Admin` und bestätigen Sie mit der OK-Taste.

3) Geben Sie das Administrator-Passwort (Standard: `123456`) ein und bestätigen Sie mit der OK-Taste.

4) Wenn Sie im internen Netz den DHCP-Server des Kommunikationssystems verwenden, überspringen Sie den nächsten Schritt.

5) Wenn Sie im internen Netz nicht den DHCP-Server des Kommunikationssystems verwenden, müssen Sie die IP-Adresse des Deployment Servers (DLS) und des Kommunikationssystems eingeben, damit die Software des IP-Systemtelefons automatisch aktualisiert werden kann. Das gilt nur für IP-Systemtelefone. Führen Sie dazu folgende Schritte durch:

- ***a)*** Blättern Sie bis `Network` und bestätigen Sie mit der OK-Taste.
- ***b)*** Blättern Sie bis `Update service (DLS)` und bestätigen Sie mit der OK-Taste.
- ***c)*** Blättern Sie bis `DLS address` und bestätigen Sie mit der OK-Taste.
- ***d)*** Geben Sie als Deployment Server die IP-Adresse des Kommunikationssystems (Standard: `192.168.1.2`) an und bestätigen Sie mit der OK-Taste.
- ***e)*** Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.
- ***f)*** Blättern Sie bis `IPv4 configuration` und bestätigen Sie mit der OK-Taste.
- ***g)*** Blättern Sie bis `Route (default)` und bestätigen Sie mit der OK-Taste.
- ***h)*** Geben Sie die IP-Adresse des Kommunikationssystems (Standard: `192.168.1.2`) an und bestätigen Sie mit der OK-Taste.
- ***i)*** Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.
- ***j)*** Navigieren Sie eine Menüebene zurück mit der Zurück-Taste.

6) Legen Sie die Rufnummer des Telefons fest:

- ***a)*** Blättern Sie bis `System` und bestätigen Sie mit der OK-Taste.
- ***b)*** Blättern Sie bis `Identity` und bestätigen Sie mit der OK-Taste.
- ***c)*** Blättern Sie bis `Terminal number` und bestätigen Sie mit der OK-Taste.
- ***d)*** Geben Sie die festgelegte Rufnummer ein (z. B. `120`) und bestätigen Sie mit der OK-Taste.
- ***e)*** Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.

7) Navigieren Sie eine Menüebene zurück mit der Zurück-Taste.

8) Wenn das Systemtelefon bedingt durch die Änderungen einen Neustart durchführen muss, erscheint in dem Menü `Admin` der Menüpunkt `Restart`. Bestätigen Sie `Restart` mit der OK-Taste und anschließend `Yes` ebenso mit der OK-Taste. Das Systemtelefon führt einen Neustart durch und meldet sich am Kommunikationssystem an.

4.9.2 Wie Sie ein SIP-Telefon konfigurieren

Voraussetzungen

- Das SIP-Telefon ist an das Kunden-LAN angeschlossen und betriebsbereit.

> ***INFO:*** Hier wird die Konfiguration am Beispiel eines OpenStage 40/60/80 SIP-Systemtelefons beschrieben. Für ein anderes SIP-Telefon müssen diese Einstellungen analog durchgeführt werden. Sehen Sie dazu bitte in der Anleitung Ihres SIP-Telefons nach.

Schritt für Schritt

1) Um in den Administrationsmodus des SIP-Systemtelefons zu gelangen, drücken Sie am Telefon die Taste für das Einstellungen-/Anwendungen-Menü.

2) Blättern Sie im Register `Einstellungen` bis `Administrator (Admin)` und bestätigen Sie mit der OK-Taste.

3) Geben Sie das Administrator-Passwort (Standard: `123456`) ein und bestätigen Sie mit der OK-Taste.

4) Wenn Sie im internen Netz den DHCP-Server des Kommunikationssystems verwenden, überspringen Sie den nächsten Schritt.

5) Wenn Sie im internen Netz nicht den DHCP-Server des Kommunikationssystems verwenden, müssen Sie die IP-Adresse des Deployment Servers (DLS) und des Kommunikationssystems eingeben, damit die Software des SIP-Systemtelefons automatisch aktualisiert werden kann. Das gilt nur für SIP-Systemtelefone. Führen Sie dazu folgende Schritte durch:

a) Blättern Sie bis `Network` und bestätigen Sie mit der OK-Taste.

b) Blättern Sie bis `Update service (DLS)` und bestätigen Sie mit der OK-Taste.

c) Blättern Sie bis `DLS address` und bestätigen Sie mit der OK-Taste.

d) Geben Sie als Deployment Server die IP-Adresse des Kommunikationssystems (Standard: `192.168.1.2`) an und bestätigen Sie mit der OK-Taste.

e) Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.

f) Blättern Sie bis `IPv4 configuration` und bestätigen Sie mit der OK-Taste.

g) Blättern Sie bis `Route (default)` und bestätigen Sie mit der OK-Taste.

h) Geben Sie die IP-Adresse des Kommunikationssystems (Standard: `192.168.1.2`) an und bestätigen Sie mit der OK-Taste.

i) Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.

j) Navigieren Sie eine Menüebene zurück mit der Zurück-Taste.

6) Legen Sie die SNTP-Zeiteinstellungen fest:

a) Blättern Sie bis `Date and time` und bestätigen Sie mit der OK-Taste.

b) Blättern Sie bis `Time source` und bestätigen Sie mit der OK-Taste.

c) Blättern Sie bis `SNTP IP address` und bestätigen Sie mit der OK-Taste.

d) Geben Sie die IP-Adresse des Kommunikationssystems (Standard: `192.168.1.2`) an und bestätigen Sie mit der OK-Taste.

e) Blättern Sie bis `Timezone offset` und bestätigen Sie mit der OK-Taste.

f) Geben Sie die Abweichung der lokalen Uhrzeit von der UTC-Zeit (Universal Time Coordinated) in Stunden an (Deutschland: `1`) und bestätigen Sie mit der OK-Taste.

g) Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.

h) Navigieren Sie eine Menüebene zurück mit der Zurück-Taste.

7) Legen Sie die Rufnummer des Telefons fest:

a) Blättern Sie bis `System` und bestätigen Sie mit der OK-Taste.

b) Blättern Sie bis `Identity` und bestätigen Sie mit der OK-Taste.

c) Blättern Sie bis `Terminal number` und bestätigen Sie mit der OK-Taste.

d) Geben Sie die festgelegte Rufnummer ein (z. B. `120`) und bestätigen Sie mit der OK-Taste.

e) Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.

8) Legen Sie die SIP-Authentifizierungsdaten fest:

a) Blättern Sie bis `Registration` und bestätigen Sie mit der OK-Taste.

b) Blättern Sie bis `SIP session` und bestätigen Sie mit der OK-Taste.

c) Notieren Sie sich die `Realm` oder geben Sie bei Bedarf eine neue Realm (z. B. `OSBIZ-SIP`) ein.

d) Notieren Sie sich die `User ID` oder geben Sie bei Bedarf eine neue User ID (z. B. `SIP-120`) ein.

e) Vergeben Sie ein `Passwort` für die Registrierung am SIP Server.

f) Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.

9) Navigieren Sie mit der Zurück-Taste zum Menü `Admin` zurück.

10) Wenn das Systemtelefon bedingt durch die Änderungen einen Neustart durchführen muss, erscheint in dem Menü `Admin` der Menüpunkt `Restart`. Bestätigen Sie `Restart` mit der OK-Taste und anschließend `Yes` ebenso mit

der OK-Taste. Das Systemtelefon führt einen Neustart durch und meldet sich am Kommunikationssystem an.

5 Erstinstallation OpenScape Business S

Beschrieben wird die Erstinstallation von OpenScape Business S (kurz Softswitch genannt). Der Softswitch und die zugehörenden Komponenten werden in das bestehende Kunden-LAN integriert. Es werden der Internet-Zugang für die Internet-Telefonie eingerichtet und die angeschlossenen Teilnehmer konfiguriert.

Für OpenScape Business S wird auf dem Linux-Betriebssystem SLES 11 SP3 64 Bit die OpenScape Business Kommunikationssoftware installiert. Die Kommunikationssoftware kann direkt auf einem Linux-Server oder in einer virtuellen Umgebung mit VMware vSphere betrieben werden. Die Installation des Linux-Betriebssystems ist beschrieben in der Installationsanleitung *OpenScape Business, Installation Linux Server*.

Die Erstinstallation von OpenScape Business S wird mit dem Administrationsprogramm OpenScape Business Assistant (Web-based Management, kurz WBM genannt) durchgeführt.

Beschrieben wird die Konfiguration der am häufigsten verwendeten Komponenten. Nicht alle dieser Komponenten werden bei Ihnen zum Einsatz kommen. Daher werden Sie bei der Erstinstallation an einigen Stellen zwischen mehreren Möglichkeiten wählen oder Konfigurationen sogar ganz überspringen müssen, je nachdem, welche Komponenten bei Ihnen Anwendung finden.

Die ausführliche Administration der über die Erstinstallation hinausgehenden Leistungsmerkmale finden Sie in den anschließenden Kapiteln.

Voraussetzung für die Erstinstallation ist die Erstellung eines IP-Adress-Schemas und eines Rufnummernplans.

Übersicht über die wichtigsten Installationsschritte:

- Systemeinstellungen
- Systemrufnummern und Vernetzung
- Internet-Telefonie
- Teilnehmer-Konfiguration
- Lizenzierung
- Datensicherung

5.1 Voraussetzungen für die Erstinstallation

Die Erfüllung der Voraussetzungen für die Erstinstallation gewährleistet den Betrieb von OpenScape Business S.

Allgemein

Abhängig von der verwendeten Hardware (Telefone,...) und der vorhandenen Infrastruktur gelten folgende allgemeine Voraussetzungen:

- Die LAN-Infrastruktur (Internet-Router, Switche, usw.) ist vorhanden und nutzbar.
- Die IP-Telefone sind an das Kunden-LAN angeschlossen.
- Der für OpenScape Business S benötigte Linux-Server wurde nach der OpenScape Business V1 Linux Server Installationsanleitung installiert, ist betriebsbereit und in das Kunden-LAN integriert.
- Alle für OpenScape Business S benötigten Lizenzen sind vorhanden (z. B. UC Clients, Gate View, Directory Services, usw...).
- Ein IP-Adressen-Schema ist vorhanden und bekannt.
- Ein Rufnummernplan ist vorhanden und bekannt.

Software

Für die Installation von OpenScape Business S wird folgende Software benötigt:

- DVD mit der OpenScape Business Kommunikationssoftware
  enthält die Kommunikationssoftware OpenScape Business. Diese DVD ist Bestandteil des Lieferumfangs.
- DVD mit Linux-Betriebssystem SLES 11 SP3 64 Bit
  Die Linux-DVD wird ggf. bei der Installation der OpenScape Business Kommunikationssoftware benötigt, wenn Software-Pakete (RPM) nachinstalliert werden müssen, die für die Kommunikationssoftware benötigt werden.

Administration

Für die Erstinstallation von OpenScape Business S mit dem OpenScape Business Assistant (WBM) kann der Linux-Server oder der Admin-PC verwendet werden. Das WBM ist browserbasiert und somit betriebssystemunabhängig.

- Webbrowser:
  Es werden nachfolgende HTML 5 fähige Web-Browser unterstützt:
  - Microsoft Internet Explorer ab Version 10 (Admin-PC)
  - Mozilla Firefox ab Version 17 (Linux-Server / Admin-PC)

  Falls eine ältere Webbrowser-Version installiert ist, muss eine aktuelle Version installiert werden, bevor mit der Erstinstallation begonnen werden kann.
- Java Runtime Environment:
  Es muss immer die aktuellste Version des Java Runtime Environments installiert sein. Ist eine ältere Version installiert, muss auf die aktuellste Version aktualisiert werden, bevor mit der Erstinbetriebnahme begonnen werden kann.
- Bildschirmauflösung: 1024x768 oder höher

Firewall

Beim Anschluss an das Internet ist für den Linux-Server eine Firewall nötig, um unautorisierten Zugriff von außen zu verhindern. Nach der Installation von Linux ist die Linux-Firewall aktiviert. Durch das Installationsprogramm der Kommunikationssoftware wird die Firewall so angepasst, dass sie den Betrieb der Kommunikationssoftware zulässt. Die Ports für die Kommunikationssoftware sind geöffnet, alle anderen Ports geschlossen.

Wird im Netzwerk eine externe Firewall eingesetzt, müssen die Linux-Firewall deaktiviert und die für die Kommunikationssoftware erforderlichen Adressen und Ports freigegeben werden (siehe *Verwendete Ports*).

Internet-Zugang

Der Server-PC benötigt einen Breitband-Internet-Zugang für:

- Sicherheits-Patches und allgemeine Linux Software-Updates

OpenScape Business benötigt einen Internet-Zugang für:

- OpenScape Business Software-Updates
- OpenScape Business Leistungsmerkmale wie z. B. Internet-Telefonie
- OpenScape Business Mobility Clients, wie z. B. myPortal for Mobile
- Remote Service (SSDP)

E-Mail-Server (optional)

OpenScape Business benötigt für das Versenden von E-Mails einen E-Mail-Server-Zugang. Hierzu sind in OpenScape Business die Zugangsdaten zum E-Mail Server und im E-Mail-Server die entsprechenden Accounts einzurichten (IP-Adresse, URL, Login-Daten des E-Mail-Servers).

Wird die E-Mail-Funktionalität innerhalb OpenScape Business nicht genutzt, müssen diese Daten nicht erfasst werden.

Internet-Telefonie, VoIP (optional)

Wird die Internet-Telefonie innerhalb OpenScape Business genutzt, benötigt OpenScape Business einen Zugang zum Breitband-Internet und zu einem Internet-Telefonie-Service Provider (ITSP, SIP-Provider) für die SIP-Telefonie über das Internet. Hierzu sind entsprechende Accounts beim ITSP zu beantragen und in OpenScape Business die Zugangsdaten zum ITSP einzurichten (IP-Adresse, URL, Login-Daten des SIP-Providers).

Zweiter LAN-Anschluss

Besitzt OpenScape Business S (bzw. der Linux-Server) einen zweiten LAN-Anschluss, können Sie diesen als WAN-Schnittstelle für den Internet-Zugang und für die Internet-Telefonie über ITSP einrichten. Der erste LAN-Anschluss dient wie gewohnt als LAN-Schnittstelle für die internen Telefone und PCs. Die Einrichtung des Internet-Zugangs erfolgt im externen Internet-Router des Kunden-LAN. Die Einrichtung des zweiten LAN-Anschlusses erfolgt direkt bei der Erstinstallation von Linux oder nachträglich über YaST. Im WBM muss der zweite LAN-Anschluss nur noch als WAN-Schnittstelle aktiviert werden.

Fax als PDF

Sollen Faxe im PDF-Format gespeichert werden, benötigt der Server-PC mindestens 4 GB RAM. Wird OpenScape Business S in einer virtuellen Umgebung betrieben, so muss dem virtuellen System ebenfalls 4 GB RAM zugewiesen werden.

5.2 Komponenten

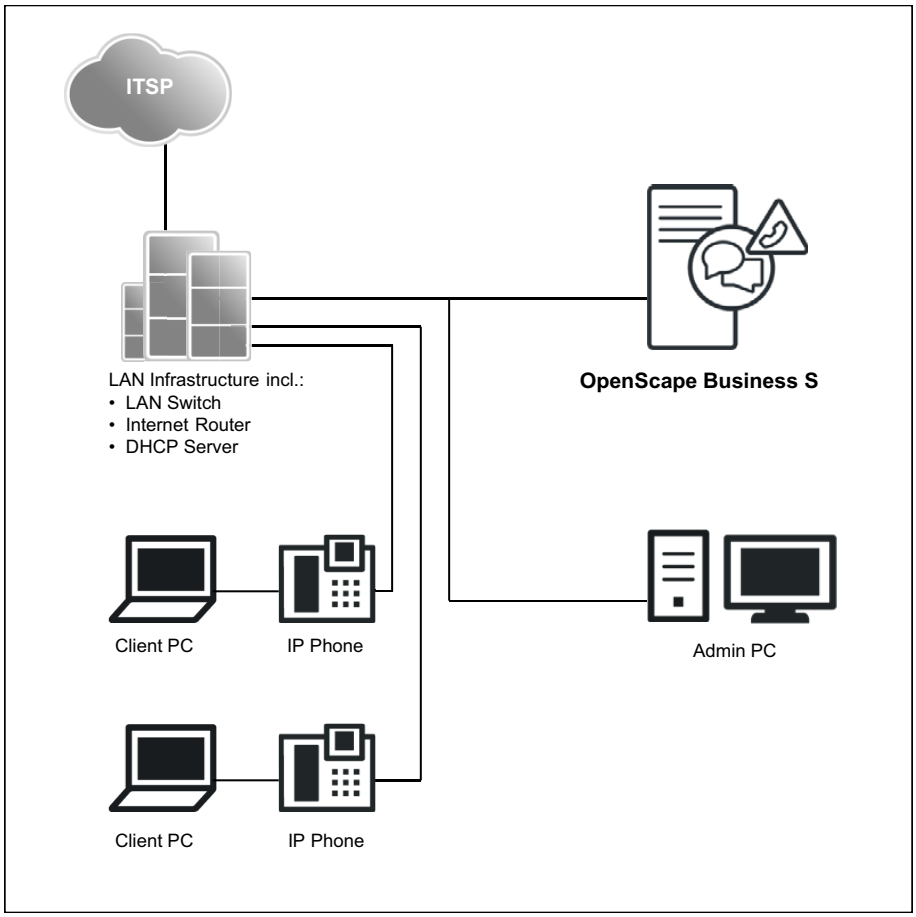
Die Komponenten des Installationsbeispiels sind im Folgenden beschrieben und skizziert.

Das Installationsbeispiel umfasst folgende Komponenten:

- OpenScape Business S
  Der Linux-Server mit der OpenScape Business S Kommunikationssoftware ist über seine LAN-Schnittstelle in das vorhandene Kunden-LAN eingebunden.
- Admin-PC
  Der Admin-PC ist ebenfalls über seine LAN-Schnittstelle in das vorhandene Kunden-LAN integriert.
- IP-Teilnehmer (IP-Clients)
  Die IP-Teilnehmer (IP-Systemtelefone, Client-PCs, WLAN Access Points, ...) sind über einen oder mehrere Switches im LAN integriert.

Die IP-Clients erhalten ihre IP-Adressen dynamisch von einem internen DHCP-Server (DHCP-Server des Linux-Servers) oder von einem externen DHCP-Server (z. B. DHCP-Server des Internet-Routers).

Der Internet-Zugang ist im Internet-Router konfiguriert.



5.3 IP-Adressen-Schema

Ein IP-Adressen-Schema ist eine Festlegung, wie die IP-Adressen im Kunden-LAN vergeben sind. Es beinhaltet die IP-Adressen von PCs, Servern, Internet-Routern, IP-Telefonen usw.

Für eine bessere Übersicht bei der Zuordnung von IP-Adressen sollte ein IP-Adressen-Schema erstellt werden.

Beispiel eines IP-Adressen-Schemas mit dem IP-Adressband `192.168.5.x`:

IP-Adressbereich	Clients
192.168.5.1 bis **192.168.5.49**	Clients mit fester IP-Adresse
192.168.5.1	Internet-Router (Gateway)
192.168.5.10	Server-PC (OpenScape Business S)
192.168.5.20	E-Mail-Server
192.168.5.100 bis **192.168.5.254**	Client-PCs & IP-Telefone, zugleich IP-Adressband des DHCP-Servers, Zuweisung der IP-Adressen an die Clients erfolgt dynamisch

5.4 Rufnummernplan

Ein Rufnummernplan ist eine Liste aller im Kommunikationssystem verfügbaren Rufnummern. Er beinhaltet interne Rufnummern, Durchwahlnummern und Gruppenrufnummern.

Standard-Rufnummernplan

Die internen Rufnummern sind mit Standardwerten vorbelegt. Diese Werte können bei Bedarf an die eigenen Belange angepasst werden (individueller Rufnummernplan).

Auszug aus dem Standard-Rufnummernplan:

Art der Rufnummern	Standard-Rufnummern
Interne Teilnehmer-Rufnummern	100-349, 500-709
Teilnehmer-Durchwahlnummern	100-349, 500-709
Gruppenrufnummern	350-439
Voicemail-Rufnummer	71
Announcement Player Rufnummer	72
Richtungskennzahlen (Externkennzahlen): Amt ITSP	 855-858

Art der Rufnummern	Standard-Rufnummern
Rufnummer für Konferenzen	7400-7404
Rufnummer für Parken	7405
Rufnummer für AutoAttendant	7410-7429
Rufnummer für MeetMe-Konferenz	7430

Individueller Rufnummernplan

Ein individueller Rufnummernplan kann im WBM während der Basiskonfiguration über eine XML-Datei importiert werden.

Die XML-Datei enthält mehrere Register. Das Register "Stations" enthält zusätzlich zu den Namen und den Rufnummern der Teilnehmer weitere Teilnehmerdaten, wie z. B. die Teilnehmer-Typen und die E-Mail-Adressen der Teilnehmer.

Ein Beispiel einer XML-Datei mit zugehöriger Erklärung finden Sie im WBM unter **Service-Center > Documente > CSV-Vorlagen**. Die dort abgelegte XML-Datei können Sie auch als Vorlage für Ihre Daten verwenden. Sie kann z. B. mit Microsoft Excel bearbeitet werden.

5.5 Installation der Kommunikationssoftware

Die OpenScape Business S Kommunikationssoftware wird auf dem Linux-Server installiert.

Achten Sie darauf, dass die zu konfigurierenden IP-Adressen und Netzmasken zu dem Kunden-LAN passen.

DHCP-Server

Ein DHCP-Server weist den IP-Teilnehmern (IP-Telefone, PCs, usw.) automatisch eine IP-Adresse zu und versorgt sie mit netzwerkspezifischen Daten, wie z.B. der IP-Adresse des Standard-Gateways.

Als DHCP-Server kann ein externer DHCP-Server genutzt werden (z.B. der DHCP-Server des Internet-Routers oder des Kommunikationssystems) oder der DHCP-Server des Linux-Servers. Soll der DHCP-Server des Linux-Servers verwendet werden, muss der externer DHCP-Server deaktiviert werden. Die Konfiguration des Linux-DHCP-Servers kann während der Installation der OpenScape Business Kommunikationssoftware durchgeführt werden.

Virtuelle Umgebung

Die Kommunikationssoftware kann in einer virtuellen Umgebung laufen. Dafür gibt es zwei Möglichkeiten der Installation:

- Getrennte Installation von Linux und Kommunikationssoftware
  Dazu wird auf dem Server-PC zuerst die Virtualisierungssoftware (Hostbetriebssystem) installiert und konfiguriert. In der virtuellen Umgebung wird Linux als Gastbetriebssystem installiert. Innerhalb des Linux-Betriebssystems wird zuletzt die Kommunikationssoftware mit Hilfe der OpenScape

Business DVD installiert (siehe hierzu *OpenScape Business V1, Linux Server, Installationsanleitung*).

- Gemeinsame Installation von Linux und Kommunikationssoftware
  Dazu wird auf dem Server-PC zuerst die Virtualisierungssoftware (Hostbetriebssystem) installiert und konfiguriert. In der virtuellen Umgebung wird ein OVA-Image installiert (Open Virtualization Appliance), dass Linux und die Kommunikationssoftware enthält. Das OVA-Image wird über den Software Supply Server (SWS) bereitgestellt.
  Bei mehr als 50 Benutzern muss nach der Installation die home-Partition auf 80 GB (50 bis 100 Benutzer) oder 180 GB (über 100 Benutzer oder bei OpenScape Business Contact Center) angepasst werden.
  Für Linux-Updates benötigen Sie zusätzlich den OpenScape Business V1 SLES Upgrade Key, um sich bei Linux registrieren zu können.

Einsatz von Snapshots auf Virtuellen Maschinen (VM):

Snapshots können ein wertvoller Wartungsmechanismus sein, z. B. um einen schnellen Rollback auf einen vordefinierten Betriebszustand der VM durchzuführen, nachdem ein Massenverteiler-Skript fehlgeschlagen ist.

- Snapshots dürfen nicht während des laufenden Betriebes durchgeführt werden. Während ein Snapshot gezogen wird, wird der aktuelle Betriebszustand der virtuellen Maschine eingefroren. Daher können verbundene Endgeräte und Applikationen, wie IP-Telefone oder die UC-Clients die Verbindung zum Server verlieren.
- Snapshots können zur Folge haben, dass interne Serverprozesse ihre Synchronisation verlieren und ein stabiler Betrieb des Kommunikationssystems nicht mehr gewährleistet ist. Daher sollte im Anschluss an den Snapshot ein Server-Neustart mit in das Wartungsfenster eingeplant werden.
- Vorherige Snapshots dürfen auf der Produktionsumgebung während des normalen Betriebes nicht verbleiben.
- Snapshots können während eines vorgesehenen Wartungsfensters oder im Rahmen der Installation gezogen werden.
- Snapshots werden intern von Backup-Tools wie VDP oder VDR genutzt. Es muss sichergestellt sein, dass diese Backup-Vorgänge außerhalb der Geschäftszeiten geplant werden und dass Snapshots, die durch diese Tools generiert werden, am Ende des Vorgangs gelöscht werden.

Weitere Informationen bezüglich Snapshots können der VMware Knowledge Base (KB) entnommen werden. Ein guter Einstiegspunkt ist der KB-Artikel 1025279 - Best Practices for virtual machine snapshots in the VMware environment (`http://kb.vmware.com/kb/1025279`).

5.5.1 Wie Sie die Kommunikationssoftware installieren

Voraussetzungen

- Das Betriebssystem SLES 11 SP3 64 Bit wurde korrekt auf dem Linux-Server installiert und gestartet.
- DVD mit OpenScape Business Kommunikationssoftware.
- DVD mit Linux-Betriebssystem SLES 11 SP3 64 Bit für die eventuell benötigte Nachinstallation von Software-Pakete (RPM).
- Die Root-Zugangsdaten (Benutzername und Passwort) für die Anmledung am Linux-Server liegen vor.

> ***WICHTIG:*** Die OpenScape Business Kommunikationssoftware überschreibt bei der Installation evtl. vorhandene Konfigurationsdateien (z. B. für DHCP, FTP, Postfix, usw.).

Schritt für Schritt

1) Melden Sie sich am Linux-Server mit Root-Rechten an.

2) Legen Sie die OpenScape Business DVD in das DVD-Laufwerk ein.

3) Bestätigen Sie den Hinweis mit **Run**. Es erscheint das Fenster "Welcome".

4) Wählen Sie die gewünschte Setup-Sprache aus (z. B. **english**) und klicken Sie auf **Start**. Die weitere Installation ist für die englische Sprachauswahl beschrieben.

5) Wählen Sie aus der Liste das gewünschte Produkt aus und klicken Sie auf **Select**. Es wird geprüft, ob die Hardware alle Voraussetzungen für die Installation erfüllt. Bei geringfügiger Unterschreitung der Voraussetzungen erfolgt eine Warnung. Nach Bestätigung kann die Installation fortgesetzt werden. Bei schwerwiegender Unterschreitung wird die Installation automatisch abgebrochen.

6) Es wird untersucht, ob zusätzliche RPM-Pakete installiert werden müssen. Falls ja, bestätigen Sie dies mit **Confirm**. Später muss in diesem Fall auf die SLES 11 DVD gewechselt werden.

7) Es erscheint ein Fenster mit den Lizenzbestimmungen (EULA, End User License Agreement). Lesen Sie sich die Lizenzbestimmungen durch und akzeptieren Sie die Lizenzbestimmungen mit **Yes**.

8) Wenn im Kunden-LAN bereits ein DHCP-Server vorhanden ist (z.B. der DHCP-Server des Internet-Routers), brechen Sie hier die Konfiguration des Linux-DHCP-Servers mit **No** ab. Fahren Sie mit Schritt 12 fort.

INFO: Damit auch bei Nutzung eines externen DHCP-Servers die Software der Systemtelefone automatisch aktualisiert werden kann, haben Sie zwei Möglichkeiten:

a) bei jedem Systemtelefon muss als DLS-Adresse die IP-Adresse des Linux-Servers eingetragen werden.

b) bei dem externen DHCP-Server müssen die netzwerkspezifischen Daten eingetragen werden. Die Parameter dazu finden Sie unter `/var/log/OPTI.txt`.

9) Wenn Sie den Linux-DHCP-Server nutzen wollen, Klicken Sie auf **Yes**, um den Linux-DHCP-Server zu aktivieren und zu konfigurieren.

10) Geben Sie folgende Werte ein (vorbelegt mit Standard-Werten):

- **Default Route**: IP-Adresse des Standard-Gateways, in der Regel die IP-Adresse des Internet-Routers, z.B. `192.168.5.1`.
- **Domain** (optional): die während der Linux-Installation angegebene Domäne, z.B. `<customer>.com`
- **DNS-Server** (optional): die während der Linux-Installation angegebene IP-Adresse des DNS-Servers. Ist im internen Netz kein DNS-Server vorhanden, können Sie hier die IP-Adresse des Internet-Routers eintragen (z. B. `192.168.5.1`).
- **SNTP Server**: IP-Adresse des internen oder externen NTP-Servers.
- **DLS/DLI Server**: IP-Adresse des DLS-Servers, d.h. die IP-Adresse des Linux-Servers (z.B. `192.168.5.10`).
- **Subnet**: das zum IP-Adressbereich passende Subnetz, z.B. `192.168.5.0`.
- **Netmask**: die während der Linux-Installation angegebene Subnetzmaske des Linux-Servers, z.B. `255.255.255.0`.
- **IP range begin** und **IP range end**: IP-Adressbereich, aus dem der DHCP-Server die IP-Adressen vergeben darf, z.B. `192.168.5.100` bis `192.168.5.254`.

11) Klicken Sie auf **Continue**.

12) Nach der Installation ist ein Neustart des Linux-Betriebssystems notwendig. Aktivieren Sie das Kontrollkästchen **PC Reboot** und bestätigen Sie mit **Continue**.

13) Wenn zusätzliche RPM-Pakete installiert werden müssen, werden Sie aufgefordert, die SLES 11 DVD einzulegen. Legen Sie die DVD ein und bestätigen Sie mit **Continue**. Legen Sie nach erfolgreicher Installation der RPM-Pakete wieder die OpenScape Business DVD ein und bestätigen Sie mit **Continue** und anschließend mit **Run**.

14) Die OpenScape Business Kommunikationssoftware wird installiert. Anschließend führt das Betriebssystem automatisch einen Neustart durch.

15) Melden Sie sich nach dem Neustart mit dem Benutzerkonto an, das zuvor bei der Linux-Installation eingerichtet wurde.

16) Klicken Sie auf dem Desktop mit der rechten Maustaste auf das Symbol des DVD-Laufwerks und wählen Sie den Menüpunkt **Eject**. Entfernen Sie die OpenScape Business DVD aus dem DVD-Laufwerk.

INFO: Es dauert einige Minuten, bis alle Komponenten der OpenScape Business Kommunikationssoftware aktiv sind. Mit dem OpenScape Observer können Sie kontrollieren, wann die OpenScape Business Kommunikationssoftware betriebsbereit ist.

5.6 Funktionskontrolle mit dem OpenScape Observer

Mit dem Programm OpenScape Observer können Sie kontrollieren, ob OpenScape Business betriebsbereit ist.

Der OpenScape Observer kann vom Admin-PC oder von einem Client-PC im internen Netz gestartet werden. Dazu muss das Programm aus dem Service-Center des WBM auf den PC kopiert werden.

5.6.1 Wie Sie den OpenScape Observer auf den PC kopieren

Voraussetzungen

- Die OpenScape Business Kommunikationssoftware ist installiert.
- Die aktuellste Java Runtime Environment Version ist auf dem PC installiert.

Schritt für Schritt

1) Starten Sie auf dem PC den Webbrowser und rufen Sie die Anmeldeseite des WBM unter folgender Adresse auf:

`https://<IP-Adresse des Linux-Servers>`, z. B. `https://192.168.5.10`.

2) Wenn der Webbrowser ein Problem mit einem Sicherheitszertifikat meldet, installieren Sie das Zertifikat (am Beispiel der Internet Explorers V10).

a) Schließen Sie den Webbrowser.

b) Öffnen Sie den Webbrowser mit Administratorrechten, indem Sie mit der rechten Maustaste auf das Webbrowser-Symbol klicken und im Kontextmenü den Eintrag **Als Administrator ausführen** auswählen.

c) Erlauben Sie die Benutzerkontensteuerung.

d) Rufen Sie die Anmeldeseite des WBM unter folgender Adresse auf:

`https://<IP-Adresse des Linux-Servers>`, z. B. `https://192.168.5.10`.

e) Klicken Sie auf **Laden dieser Website fortsetzen**.

f) Klicken Sie auf die Meldung **Zertifikatsfehler** in der Navigationsleiste des Webbrowsers.

g) Klicken Sie auf **Zertifikate anzeigen**.

h) Klicken Sie auf **Zertifikat installieren** (nur sichtbar mit Administratorrechten).

i) Wählen Sie die Option **Lokaler Computer** und bestätigen Sie mit **Weiter**.

j) Wählen Sie die Option **Alle Zertifikate in folgendem Speicher speichern**, klicken Sie auf **Durchsuchen** und geben Sie **Vertrauenswürdige Stammzertifizierungsstellen** an.

k) Bestätigen Sie mit **OK** und anschließend mit **Weiter** und **Fertigstellen**.

l) Bestätigen Sie den Zertifikatimport mit **OK** und schließen Sie das Zertifikatsfenster mit **OK**.

m) Schließen Sie den Webbrowser.

n) Starten Sie den Webbrowser erneut (ohne Administratorrechte) und rufen Sie die Anmeldeseite des WBM unter folgender Adresse auf:

`https://<IP-Adresse des Linux-Servers>`, z. B. `https://192.168.5.10`.

3) Klicken Sie oben rechts auf das Sprachkürzel und wählen Sie aus dem Menü die Sprache aus, in der die Oberfläche des WBM angezeigt werden soll. Die Anmeldeseite wird in der ausgewählten Sprache angezeigt.

4) Geben Sie im ersten Feld unter **Login** den Standard-Benutzernamen `administrator@system` für den Zugang als Administrator ein.

> ***INFO:*** Wenn Sie nach der Eingabe von `administrator` die Tabulator-Taste drücken, wird `@system` automatisch ergänzt.

5) Geben Sie im zweiten Feld unter **Login** das Standard-Passwort `administrator` für den Zugang als Administrator ein.

6) Klicken Sie auf **Login**.

7) Sie werden aufgefordert, das Standard-Passwort zu ändern.

a) Geben Sie im Feld **Passwort** nochmal das Standard-Passwort `administrator` ein.

b) Geben Sie in den Feldern **Neues Passwort** und **Neues Passwort bestätigen** ein neues Passwort ein, um das System gegen Missbrauch zu schützen. Berücksichtigen Sie Groß-/Kleinschreibung und den Zustand der Taste **Num**. Das Passwort erscheint verdeckt durch Sternchen (*).

> ***INFO:*** Das Passwort muss mindestens 8 Zeichen lang sein und eine Ziffer enthalten. Bitte merken Sie sich Ihr neues Passwort genau.

8) Klicken Sie auf **Login**.

9) Klicken Sie in der Navigationsleiste auf **Service-Center**.

10) Klicken Sie im Bereich **Software** auf den Eintrag **OpenScape Observer**.

11) Speichern Sie die Datei `OsoObserver.jar` auf dem PC in einem Verzeichnis Ihrer Wahl.

5.6.2 Wie Sie den OpenScape Observer vom PC starten

Voraussetzungen

- Die Datei `OsoObserver.jar` ist auf dem Client-PC abgelegt.

Schritt für Schritt

1) Navigieren Sie auf dem PC zum Ablagepfad des OpenScape Observers.

2) Doppelklicken Sie auf die Datei `OsoObserver.jar`. Der OpenScape Observer öffnet sich als kleines Fenster in der linken oberen Ecke des Bildschirms.

3) Geben Sie im Feld des OpenScape Observers die IP-Adresse des Linux-Servers ein, auf dem die OpenScape Business Kommunikationssoftware installiert ist (z. B. `192.168.5.10`).

4) Klicken Sie auf **Connect OSO**.

5) Es öffnet sich ein weiteres Fenster mit folgendem Inhalt:

- IP-Adresse des Linux-Servers (in der Kopfzeile)
- Versionsnummer der installierten OpenScape Business Kommunikationssoftware
- Version des Linux-Server-Betriebssystems
- Auslastung der home-Partition (`HD`) und des Arbeitsspeichers (`RAM`) des Linux-Servers in Prozent
- Abkürzung des installierten Produkts (z. B. `S` für OpenScape Business S und `B` für UC Booster Server)

6) In dem Fenster werden Sie zusätzlich mit einer LED-Anzeige über den Status von OpenScape Business informiert:

- Rote LED: Die OpenScape Business Systemkomponenten können nicht gestartet werden - OpenScape Business ist nicht betriebsbereit
- Gelbe LED: Die OpenScape Business Systemkomponenten werden gestartet - OpenScape Business ist noch nicht betriebsbereit
- Grüne LED: Die OpenScape Business Systemkomponenten sind gestartet - OpenScape Business ist betriebsbereit

5.7 Inbetriebnahme

Mit dem Wizard **Erstinstallation** des WBM werden die grundlegenden Einstellungen durchgeführt.

5.7.1 Wie Sie den Wizard Erstinstallation starten

Voraussetzungen

- Das WBM ist gestartet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie auf **Bearbeiten**, um den Wizard **Erstinstallation** zu starten.

> ***INFO:*** Wenn bei niedrigen Bildschirmauflösungen der Arbeitsbereich aufgrund der Größe des Browserfensters nicht komplett angezeigt werden kann, so erscheinen horizontale oder vertikale Rollbalken an den Rändern, mit denen der angezeigte Ausschnitt verschoben werden kann.

Nächste Schritte

Führen Sie die Erstinstallation wie nachstehend beschrieben Schritt für Schritt durch. Felder, die hier nicht beschrieben werden, sind passend für den Standardfall vorbelegt und müssen nur geändert werden, wenn sie nicht zu Ihren Netzwerkdaten passen. Die ausführlichen Informationen finden Sie in der Administratordokumentation bei der Beschreibung der einzelnen Wizards.

5.7.2 Systemeinstellungen

Im Fenster **Systemeinstellungen** konfigurieren Sie die Systemeinstellungen des Kommunikationssystems.

Gehen Sie folgendermaßen vor:

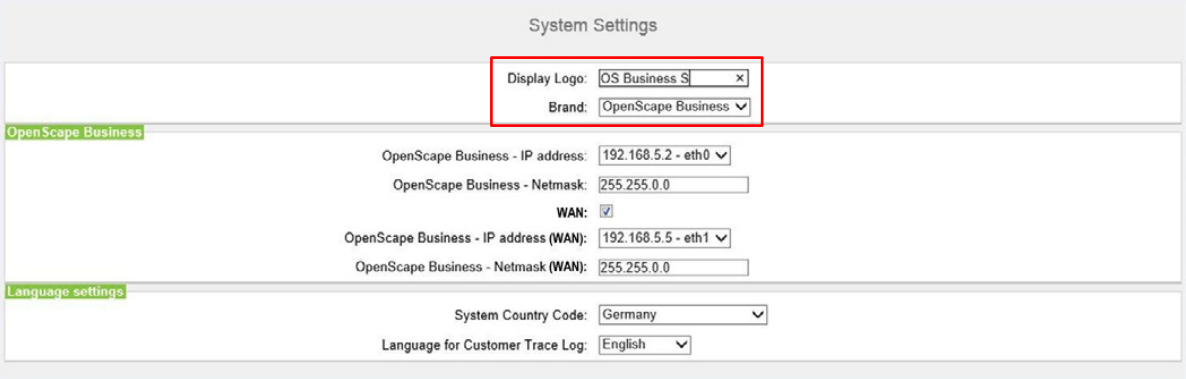
1. Display-Logo und Produktbezeichnung festlegen
   Sie können einen Display-Text festlegen, das im Display der Systemtelefone angezeigt wird. Zusätzlich können Sie die Produktbezeichnung auswählen.
2. Länderkennzeichen und Sprache für Event-Logs auswählen
   Für eine korrekte Länderinitialisierung müssen Sie das Land auswählen, in dem das Kommunikationssystem betrieben wird. Zusätzlich können Sie die Sprache auswählen, in der die Event-Logs (Protokolle für Systemereignisse, Fehler, usw.) abgespeichert werden.

3. Nur bei Bedarf: weiteren LAN-Anschluss als WAN-Schnittstelle aktivieren
   Besitzt OpenScape Business S (bzw. der Linux-Server) einen zweiten LAN-Anschluss, können Sie diesen als WAN-Schnittstelle für den Internet-Zugang und für die Internet-Telefonie über ITSP einrichten. Der erste LAN-Anschluss dient wie gewohnt als LAN-Schnittstelle für die internen Telefone und PCs.

5.7.2.1 Wie Sie das Display-Logo und die Produktbezeichnung festlegen

Voraussetzungen

- Sie befinden sich im Fenster **Systemeinstellungen**.



Schritt für Schritt

1) Geben Sie im Feld **Display-Logo** einen Text Ihrer Wahl ein (z. B. OS Business S). Der Text kann bis zu 16 Zeichen lang sein. Vermeiden Sie Umlaute und Sonderzeichen.

2) Wählen Sie in der Aufklappliste **Produkt** die Produktbezeichnung aus.

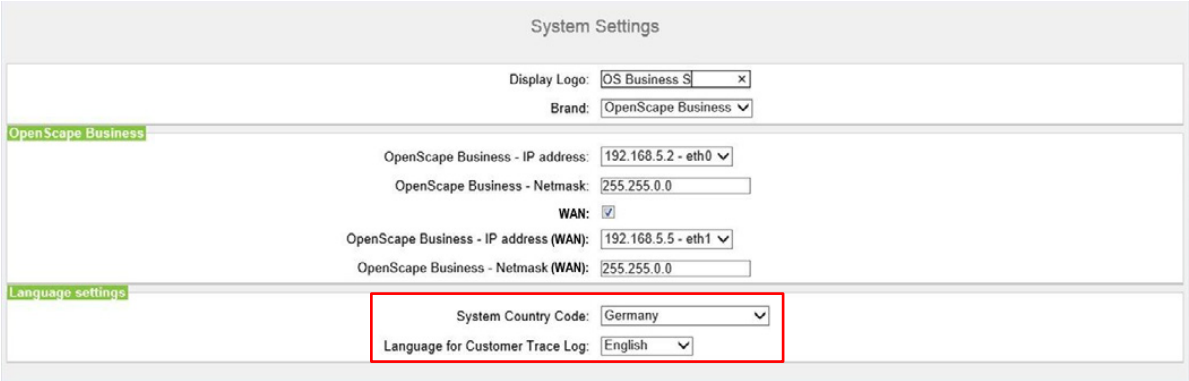
Nächste Schritte

Länderkennzeichen und Sprache für die Event-Logs auswählen.

5.7.2.2 Wie Sie das Länderkennzeichen und die Sprache für Event-Logs auswählen

Voraussetzungen

- Sie befinden sich im Fenster **Systemeinstellungen**.



Schritt für Schritt

1) Wählen Sie in der Aufklappliste **System-Länderkennzeichen** das Land aus, in dem das Kommunikationssystem betrieben wird.

2) Wählen Sie im Feld **Sprache für Kunden-Eventlog** die Sprache aus, in der die Event-Logs (Protokolle für Systemereignisse, Fehler, usw.) ausgegeben werden sollen.

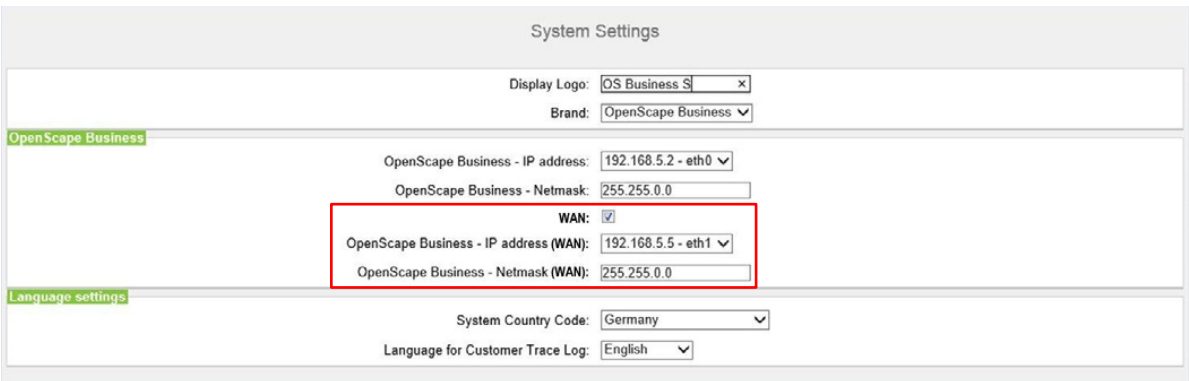
Nächste Schritte

Basiskonfiguration starten.

5.7.2.3 Wie Sie einen weiteren LAN-Anschluss als WAN-Schnittstelle aktivieren

Voraussetzungen

- Sie befinden sich im Fenster **Systemeinstellungen**.



Schritt für Schritt

1) Aktivieren Sie das Kontrollkästchen **WAN**.

2) Wählen Sie aus der Aufklappliste **OpenScape Business - IP-Adresse (WAN)** den gewünschten LAN-Anschluss aus (z. B. `eth1` oder `eth2`). Sind nur zwei LAN-Anschlüsse vorhanden, wird automatisch der zweite LAN-Anschluss `eth1` aktiviert.

INFO: Die Zuordnung der IP-Adressen und Subnetz-Masken zu den LAN-Anschlüssen erfolgt während der Erstinstallation von Linux oder nachträglich über YaST.

Nächste Schritte

Basiskonfiguration starten.

5.8 Basiskonfiguration

Die Basiskonfiguration wird mit dem Wizard **Basisinstallation** des WBM durchgeführt. Dabei werden die wichtigsten Einstellungen für den Betrieb des Kommunikationssystems festgelegt.

5.8.1 Wie Sie den Wizard Basisinstallation starten

Voraussetzungen

- Der Wizard **Erstinstallation** ist durchlaufen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie auf **Bearbeiten**, um den Wizard **Basisinstallation** zu starten.

Nächste Schritte

Führen Sie die Basisinstallation wie nachstehend beschrieben Schritt für Schritt durch. Felder, die hier nicht beschrieben werden, sind passend für den Standardfall vorbelegt und müssen nur geändert werden, wenn sie nicht zu Ihren Netzwerkdaten passen. Die ausführlichen Informationen finden Sie in der Administratordokumentation bei der Beschreibung der einzelnen Wizards.

5.8.2 Systemrufnummern und Vernetzung

Im Fenster **Übersicht** geben Sie die Systemrufnummern ein (Anlagenrufnummer, Länder- und Ortsvorwahl, Internationales Präfix) und legen fest, ob OpenScape Business mit anderen OpenScape Business Systemen vernetzt werden soll.

Gehen Sie folgendermaßen vor:

1. Systemrufnummern eingeben

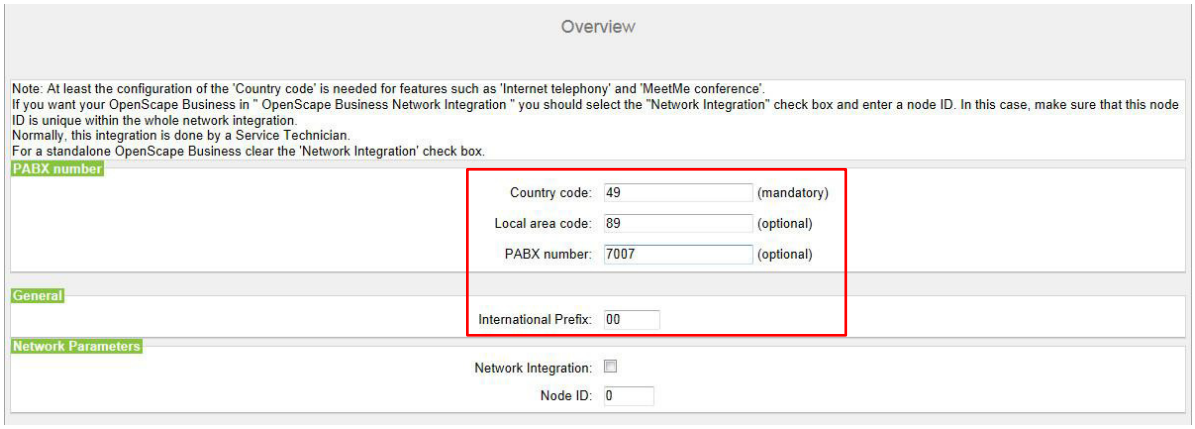
- Systemrufnummern für Anlagenanschluss eingeben
  Hier geben Sie die Anlagenrufnummer für Ihren Anlagenanschluss ein sowie die Länder- und Ortsvorwahl.
  Die Eingabe der Ländervorwahl ist für Internet-Telefonie und Konferenz-Server-Funktionalitäten zwingend erforderlich.
  Das internationale Präfix ist abhängig von der zuvor gewählten Länderkennzahl vorbelegt.
- Systemrufnummern für Mehrgeräteanschluss eingeben
  Hier geben Sie Länder- und Ortsvorwahl für Ihren Mehrgeräteanschluss ein.
  Die Eingabe der Ländervorwahl ist für Internet-Telefonie und für MeetMee-Konferenzen zwingend erforderlich.
  Das internationale Präfix ist abhängig von der zuvor gewählten Länderkennzahl vorbelegt.

2. Vernetzung aktivieren oder deaktivieren
   Soll OpenScape Business mit anderen OpenScape Business Systemen vernetzt werden, muss die Vernetzung aktiviert und OpenScape Business eine Knoten-ID zugewiesen werden. Jede OpenScape Business muss im Netzverbund eine eindeutige Knoten-ID besitzen.

5.8.2.1 Wie Sie die Systemrufnummern für einen Anlagenanschluss eingeben

Voraussetzungen

- Sie haben einen Anlagenanschluss.
- Sie befinden sich im Fenster **Übersicht**.



Schritt für Schritt

1) Geben Sie im Feld **Ländervorwahl** die Ländervorwahl ein, z. B. `49` für Deutschland oder `1` für USA.

2) Geben Sie im Feld **Ortsnetzkennzahl** die Ortsvorwahl ein, z. B. `89` für München.

3) Geben Sie im Feld **Anlagenrufnummer** die Anlagenrufnummer Ihres Amtsanschlusses ein, z. B. `7007` (Ihre Anschlussnummer).

4) Ändern Sie das Feld **Internationales Präfix** nur wenn nötig. Für Deutschland gilt `00`, für USA `011`).

Bei Telefonaten ins Ausland wird der Telefonnummer das internationale Präfix und die Ländervorwahl vorangestellt, z. B. bei einem Telefonat von Deutschland nach USA die "00-1-..." und bei einem Telefonat von USA nach Deutschland die "011-49-...".

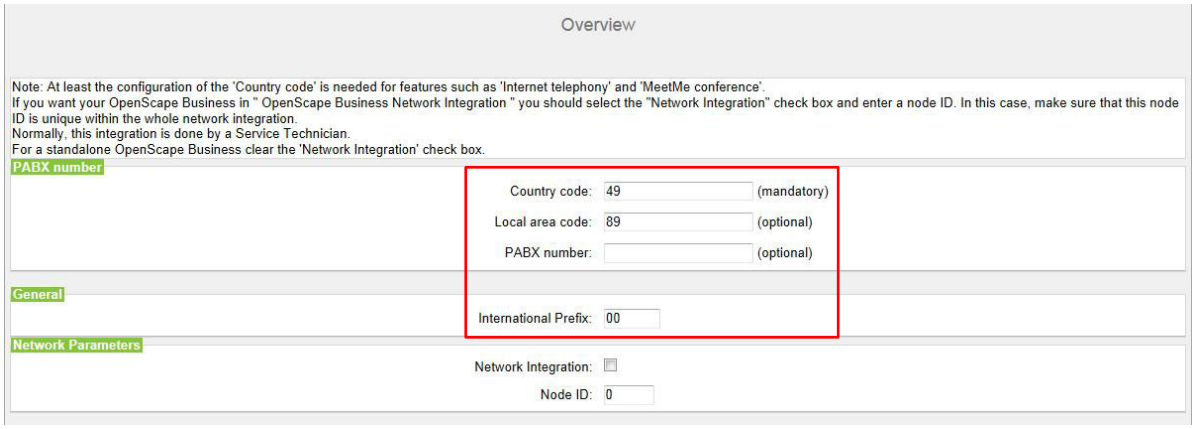
Nächste Schritte

Vernetzung aktivieren oder deaktivieren.

5.8.2.2 Wie Sie die Systemrufnummern für einen Mehrgeräteanschluss eingeben

Voraussetzungen

- Sie haben einen Mehrgeräteanschluss.
- Sie befinden sich im Fenster **Übersicht**.



Schritt für Schritt

1) Geben Sie im Feld **Ländervorwahl** die Ländervorwahl ein, z. B. `49` für Deutschland oder `1` für USA.

2) Geben Sie im Feld **Ortsnetzkennzahl** die Ortsvorwahl ein, z. B. `89` für München.

3) Lassen Sie das Feld **Anlagenrufnummer** leer.

4) Ändern Sie das Feld **Internationales Präfix** nur wenn nötig. Für Deutschland gilt `00`, für USA `011`).

Bei Telefonaten ins Ausland wird der Telefonnummer das internationale Präfix und die Ländervorwahl vorangestellt, z. B. bei einem Telefonat von Deutschland nach USA die "00-1-..." und bei einem Telefonat von USA nach Deutschland die "011-49-...".

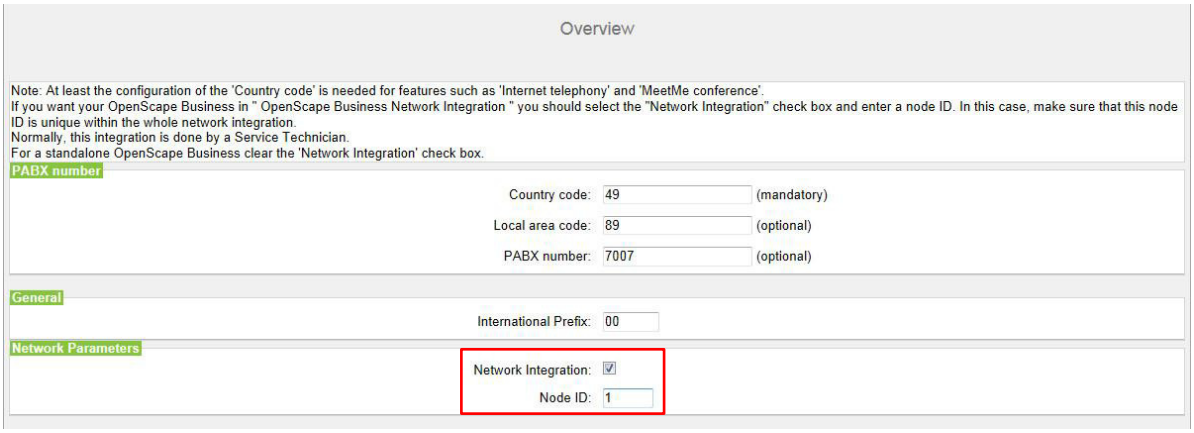
Nächste Schritte

Vernetzung aktivieren oder deaktivieren.

5.8.2.3 Wie Sie die Vernetzung aktivieren oder deaktivieren

Voraussetzungen

- Sie befinden sich im Fenster **Übersicht**.



Schritt für Schritt

1) Wenn das Kommunikationssystem mit anderen Kommunikationssystemen vernetzt werden soll:

a) Aktivieren Sie das Kontrollkästchen **Netzwerk-Integration**.

b) Vergeben Sie im Feld **Knoten-ID** für das Kommunikationssystem eine im Netzverbund eindeutige Knoten-ID (Ziffern von `1` bis `100` möglich).

2) Wenn das Kommunikationssystem nicht mit anderen Kommunikationssystemen vernetzt werden soll, lassen Sie das Kontrollkästchen **Netzwerk-Integration** deaktiviert.

3) Klicken Sie auf **OK & Weiter**.

Nächste Schritte

Teilnehmerdaten konfigurieren.

5.8.3 Teilnehmerdaten

Im Fenster **Zentrale Teilnehmer-Funktionen** können Sie bei Bedarf anstelle des vordefinierten Standardrufnummernplans Ihren individuellen Rufnummernplan konfigurieren und weitere Teilnehmerdaten importieren. Im Netzverbund muss der Standard-Rufnummernplan an den Rufnummernplan des Netzverbunds angepasst werden.

Der Standardrufnummernplan enthält vordefinierte Rufnummern für verschiedene Teilnehmertypen (IP-Telefone, analoge Telefone, ...) und für spezielle Funktionen (Internet-Telefonie, Sprachbox, AutoAttendant, ...).

Die Teilnehmerdaten enthalten u.a. die internen Rufnummern, die Durchwahlnummern und die Namen der Teilnehmer. Über eine XML-Datei im UTF-8-Format können diese Daten und weitere Teilnehmerdaten während der Basiskonfiguration in das Kommunikationssystem importiert werden.

INFO: Eine XML-Vorlage mit zugehöriger Erklärung finden Sie im WBM unter **Service-Center > Dokumente > CSV-Vorlagen**. In diese Vorlage können Sie z. B. mit Microsoft Excel Ihre Daten eintragen.

Sie haben folgende Möglichkeiten:

- **Teilnehmerdaten ohne Netzverbund konfigurieren**
  Gehen Sie folgendermaßen vor:

  a) Teilnehmerdaten anzeigen
  Sie können sich alle vorkonfigurierten Rufnummern und Teilnehmerdaten anzeigen lassen.

  b) Alle Rufnummern löschen (optional)
  Verwenden Sie einen individuellen Rufnummernplan, müssen Sie alle vorkonfigurierten Rufnummern löschen.

  c) Vorkonfigurierte Rufnummern an den individuellen Rufnummernplan anpassen (optional)
  Verwenden Sie einen individuellen Rufnummernplan, können Sie die vorkonfigurierten Rufnummern an den eigenen Rufnummernplan anpassen.

  d) Teilnehmerdaten über XML-Datei importieren (optional)
  Ihre individuellen Rufnummern inkl. zusätzlicher Teilnehmerdaten können Sie bequem über eine XML-Datei während der Basiskonfiguration importieren.

- **Teilnehmerdaten mit Netzverbund konfigurieren**
  Gehen Sie folgendermaßen vor:

  a) Alle Rufnummern löschen
  Falls im Netzverbund die UC Suite zum Einsatz kommt, ist ein geschlossener Rufnummernplan erforderlich, d.h. alle Rufnummern im Netzverbund müssen eindeutig sein. Daher müssen die vorkonfigurierten Rufnummern gelöscht und an den Netzverbund angepasste Rufnummern verwendet werden.

  b) Teilnehmerdaten über XML-Datei importieren
  Die an den Netzverbund angepassten Rufnummern sind inkl. zusätzlicher Teilnehmerdaten bequem über eine XML-Datei während der Basiskonfiguration zu importieren. Diese Datei kann alle Teilnehmer des Netzverbundes enthalten. Beim Import werden nur die Rufnummern und Teilnehmerdaten übernommen, die der zuvor angegebenen Knoten-ID des Kommunikationssystems zugeordnet sind.

5.8.3.1 Wie Sie die Teilnehmerdaten anzeigen

Voraussetzungen

- Sie befinden sich im Fenster **Zentrale Teilnehmer-Funktionen**.

Schritt für Schritt

1) Aktivieren Sie das Optionsfeld **Teilnehmerkonfiguration anzeigen**.

2) Klicken Sie auf **Funktion ausführen**. Es wird Ihnen eine Liste der Teilnehmer mit den vorkonfigurierten Rufnummern (Standard-Rufnummernplan) angezeigt.

3) Klicken Sie auf **OK**. Sie werden zum Fenster **Zentrale Teilnehmer-Funktionen** zurückgeführt.

4) Wenn Sie keine Teilnehmerdaten ändern wollen, klicken Sie auf **OK & Weiter**.

5.8.3.2 Wie Sie alle Rufnummern löschen

Voraussetzungen

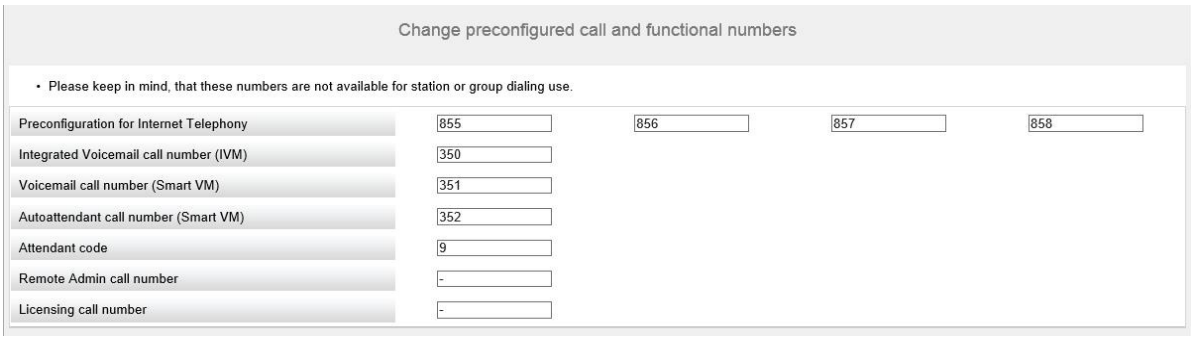
- Sie befinden sich im Fenster **Zentrale Teilnehmer-Funktionen**.

Schritt für Schritt

1) Aktivieren Sie das Optionsfeld **Alle Rufnummern löschen**.

2) Aktivieren Sie das Kontrollkästchen **Alle Rufnummern löschen**.

3) Klicken Sie auf **Funktion ausführen**. Alle vorbelegten Rufnummern werden gelöscht. Anschließend erscheint das Fenster **Vorkonfigurierte Rufnummern ändern**.



4) Passen Sie die Kennzahlen und speziellen Rufnummern an Ihre Wünsche an und klicken Sie anschließend auf **OK**. Sie werden zum Fenster **Zentrale Teilnehmer-Funktionen** zurückgeführt.

5) Wenn Sie keine weiteren Teilnehmerdaten ändern wollen, klicken Sie auf **OK & Weiter**.

5.8.3.3 Vorkonfigurierte Rufnummern an den individuellen Rufnummernplan anpassen

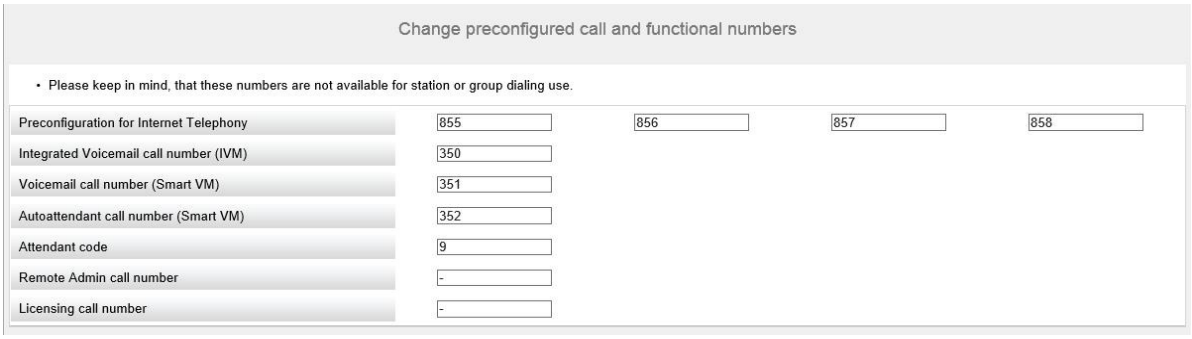
Voraussetzungen

- Sie befinden sich im Fenster **Zentrale Teilnehmer-Funktionen**.

Schritt für Schritt

1) Aktivieren Sie das Optionsfeld **Vorkonfigurierte Rufnummern ändern**.

2) Klicken Sie auf **Funktion ausführen**. Es erscheint das Fenster **Vorkonfigurierte Rufnummern ändern**.



3) Passen Sie die vorkonfigurierten Rufnummern an Ihre Wünsche an und klicken Sie anschließend auf **OK**. Sie werden zum Fenster **Zentrale Teilnehmer-Funktionen** zurückgeführt.

4) Wenn Sie keine weiteren Teilnehmerdaten ändern wollen, klicken Sie auf **OK & Weiter**.

5.8.3.4 Wie Sie die Teilnehmerdaten über eine XML-Datei importieren

Voraussetzungen

- Sie befinden sich im Fenster **Zentrale Teilnehmer-Funktionen**.
- Eine XML-Datei im UTF-8-Format mit den eingetragenen Daten liegt vor. Eine XML-Vorlage finden Sie unter **Service-Center > Dokumente > CSV-Vorlagen**.

Schritt für Schritt

1) Aktivieren Sie das Optionsfeld **XML-Datei mit Teilnehmerdaten importieren**.

2) Klicken Sie auf **Funktion ausführen**.

3) Wählen Sie mit **Durchsuchen** die erstellte XML-Datei aus und klicken Sie auf **Öffnen**.

4) Klicken Sie anschließend auf **OK**. Die Teilnehmerdaten werden importiert.

5) Klicken Sie auf **OK & Weiter**.

5.8.4 Internet-Telefonie

Im Fenster **Provider-Konfiguration und -Aktivierung für Internet-Telefonie** konfigurieren Sie die Internet-Telefonie. Sie können vorkonfigurierte oder neue Internet-Telefonie-Service-Provider (ITSP) konfigurieren. Für jeden ITSP können Sie einen oder mehrere Accounts konfigurieren. Es können bis zu 4 ITSP gleichzeitig aktiv sein.

Sie haben folgende Möglichkeiten:

- **Vordefinierten ITSP konfigurieren**
  Sie können vordefinierte ITSP-Vorlagen verwenden. Dazu werden in diese Vorlage die eigenen Zugangsdaten und Rufnummern eingetragen und diese anschließend aktiviert.
- **Neuen ITSP konfigurieren**
  Sie können auch neue ITSP hinzufügen und aktivieren.
  Einen neuen ITSP zu konfigurieren ist nur in seltenen Fällen nötig und sehr aufwändig. Deshalb wird diese Möglichkeit nicht in der Erstinstallation beschrieben. Genauere Informationen finden Sie im Kapitel *Konfiguration eines ITSP*.
- **Internet-Telefonie deaktivieren**
  Sie können die Internet-Telefonie deaktivieren.

INFO: Einrichtebeispiele finden Sie im wiki unter http://wiki.unify.com/images/1/1e/OSBiz_V1_Configuration_for_ITSP.pdf

---

Zuordnung der ITSP-Rufnummern

- Bei einem **Internet-Telefonie-Teilnehmeranschluss** stellt der ITSP Einzelrufnummern zur Verfügung, z. B. 70005555, 70005556, ... Diese Einzelrufnummern werden anschließend den internen Rufnummern der Teilnehmer manuell zugeordnet.
- Bei einem **Internet-Telefonie-Anlagenanschluss** stellt der ITSP ein Rufnummernband (Rufnummernbereich) zur Verfügung, z. B. (+49) 89 7007-100 bis (+49) 89 7007-147. Die Rufnummern aus dem Rufnummernband werden anschließend den internen Rufnummern der Teilnehmer manuell zugeordnet.

Die beiden Anschlussarten können kombiniert werden.

Alternativ können für beide Anschlussarten die ITSP-Rufnummern bei der Teilnehmer-Konfiguration als Durchwahlrufnummern der Teilnehmer eingetragen werden.

interne Rufnummer	Name	DuWa
100	Andreas Richter	897007100
101	Susanne Mueller	897007101

interne Rufnummer	Name	DuWa
102	Buddy Miller	897007102
104	Juan Martinez	70005555
105	Emilio Carrara	70005556

Somit ergeben sich die ITSP-Rufnummern aus der eingerichteten Anlagenrufnummer (z. B. Länderkennzahl 49) und den eingetragenen Durchwahlnummern im Langformat. Das hat Vorteile bei der Wahlbewertung und dem Call-Management, auch in einem Netzverbund. So ist der ITSP-Anschluss z. B. durchwahlfähig zu einem anderen Knoten.

Ein weiterer Amtsanschluss über ISDN ist in diesem Fall nur eingeschränkt möglich (sinnvoll z. B. für Notrufe).

5.8.4.1 Wie Sie einen vordefinierten ITSP konfigurieren

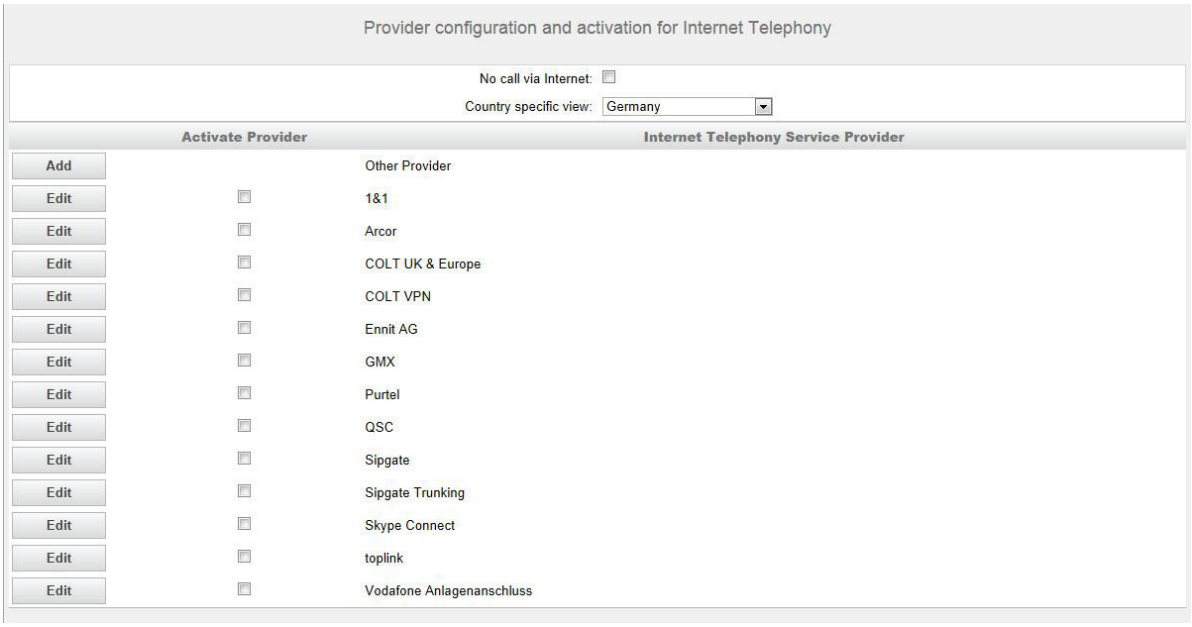
Voraussetzungen

- Sie befinden sich im Fenster **Provider-Konfiguration und -Aktivierung für Internet-Telefonie**.
- Die Verbindung zum Internet ist betriebsbereit.
- Die Internet-Telefonie-Zugangsdaten Ihres ITSP liegen Ihnen vor (z. B. Benutzerkennung, Passwort, Internet-Telefonie-Rufnummern).

Schritt für Schritt

1) Deaktivieren Sie das Kontrollkästchen **Keine Telefonie über Internet**. Es wird Ihnen eine landesabhängige Liste der möglichen ITSP angezeigt. Die

Liste enthält die für das gewählte Land vordefinierten ITSP und die eventuell bereits angelegten ITSP.



2) Wenn Sie das voreingestellte Land ändern möchten, wählen Sie aus der Aufklappliste **Länderspezifische Ansicht** das gewünschte Land aus. Es werden die für das gewählte Land möglichen ITSP angezeigt.

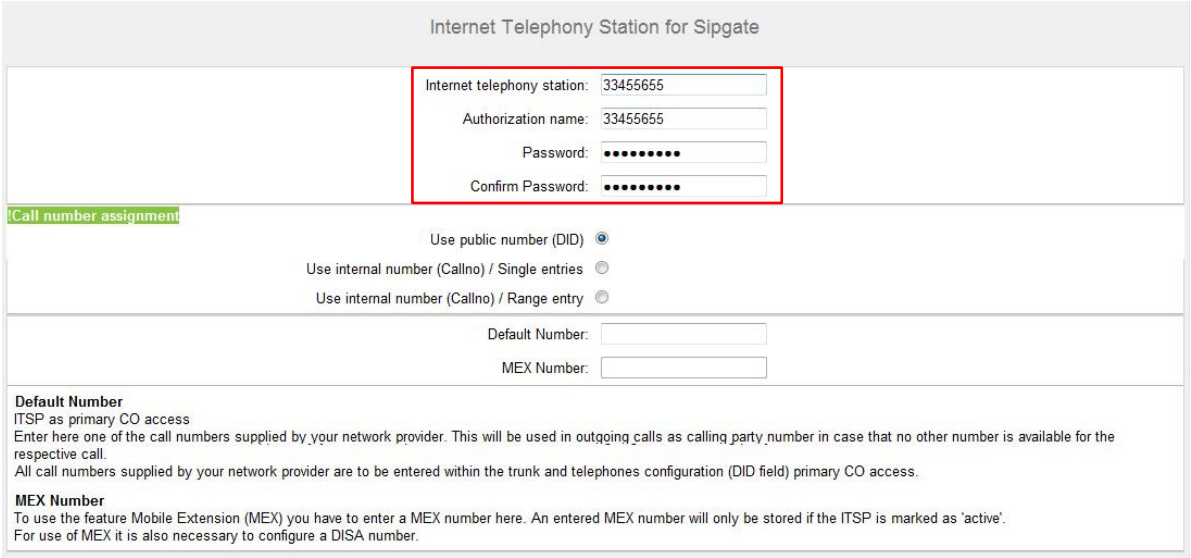
3) Klicken Sie bei Bedarf auf **Status anzeigen**, um abzufragen, welche ITSP bereits aktiviert sind und welche Internet-Telefonie-Teilnehmer unter dem jeweiligen ITSP bereits eingerichtet sind. Maximal können Sie vier ITSP aktivieren. Klicken Sie anschließend auf **OK**.

4) Klicken Sie in der Zeile des entsprechenden ITSP auf **Bearbeiten**, um einen vordefinierten ITSP zu konfigurieren.

5) Aktivieren Sie das Kontrollkästchen **Provider aktivieren**.

6) Klicken Sie auf **OK & Weiter**.

7) Klicken Sie auf **Hinzufügen**, um Ihre ITSP-Accounts mit den dazugehörigen Internet-Telefonie-Rufnummern zu konfigurieren. Die Felder, die Ihnen anschließend angezeigt werden, sind providerabhängig.



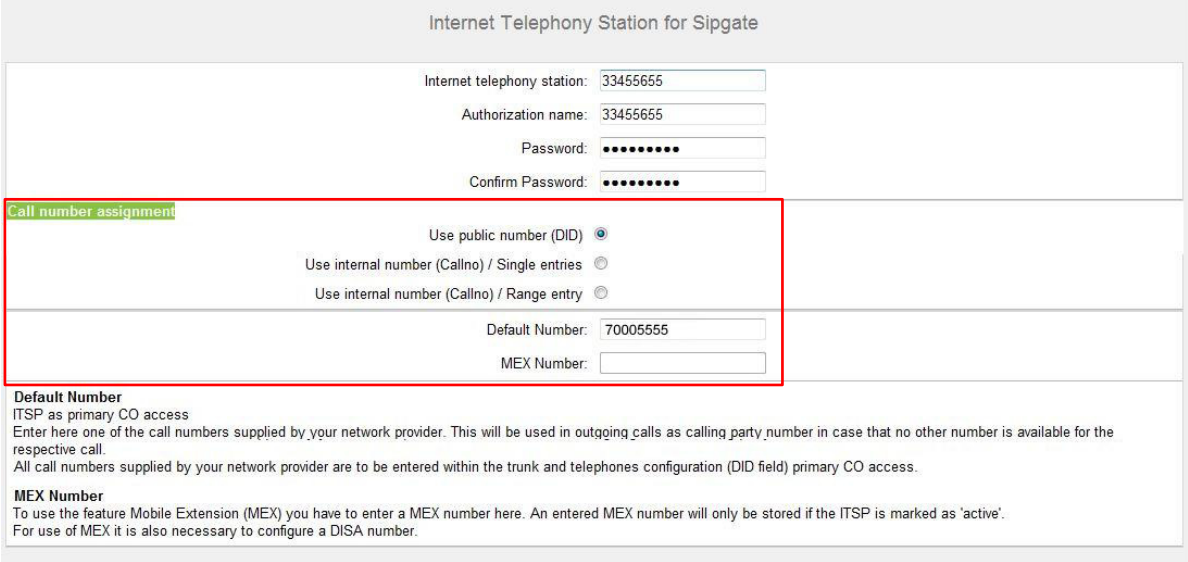
8) Geben im Feld **Internet-Telefonie-Teilnehmer** die Zugangsdaten Ihres Accounts ein. Die Daten haben Sie von Ihrem ITSP erhalten. Je nach ITSP werden hierfür unterschiedliche Bezeichnungen verwendet, wie z. B. SIP-User, SIP-Nutzer, SIP-ID.

9) Geben Sie im Feld **Autorisierungsname** den Autorisierungsnamen ein. Die Daten haben Sie von Ihrem ITSP erhalten. Haben Sie keinen Autorisierungsnamen erhalten, geben Sie die gleichen Daten wie unter **Internet-Telefonie-Teilnehmer** ein.

10) Geben Sie in den Feldern **Neues Kennwort** und **Kennwort wiederholen** das Kennwort an, dass Sie vom ITSP erhalten haben. Je nach ITSP werden hierfür unterschiedliche Bezeichnungen verwendet, wie z. B. SIP-Passwort oder SIP-Kennwort.

11) Zuordnung der Internet-Telefonie-Rufnummern - Möglichkeit 1:

Öffentliche Rufnummer (DuWa): die Internet-Telefonie-Rufnummern Ihres Internet-Telefonie-Teilnehmeranschlusses oder Internet-Telefonie-Anlagenanschlusses werden nicht hier bei der ITSP-Konfiguration, sondern bei der Teilnehmer-Konfiguration in den Feldern **DuWa** eingetragen.



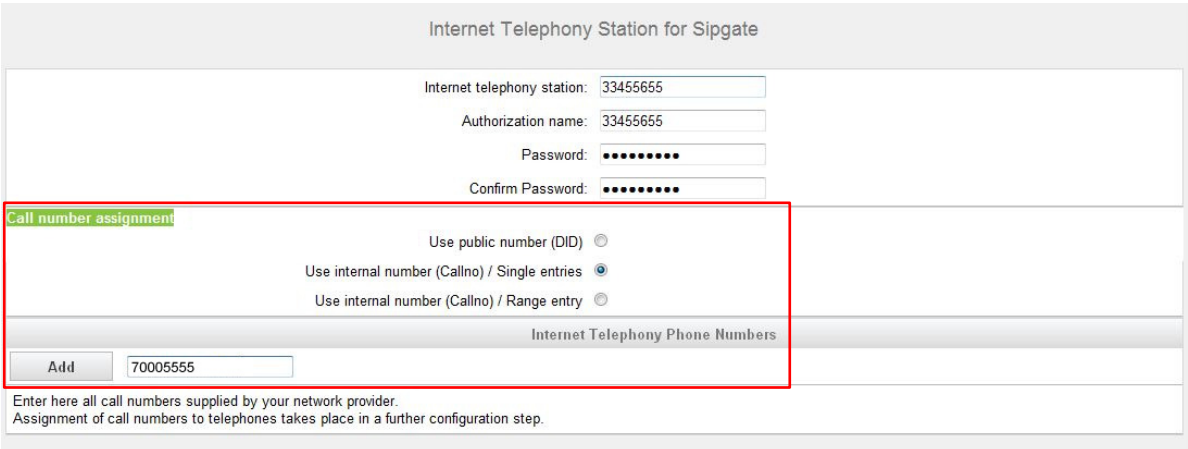
a) Wählen Sie im Bereich **Rufnummer assignment** das Optionsfeld **Öffentliche Rufnummer (DuWa)** aus.

b) Geben Sie unter **Standard-Rufnummer** die Rufnummer ein, die bei gehenden Anrufen für Teilnehmer verwendet werden soll, die keine eigene Rufnummer haben.

c) Falls Ihr ITSP das Leistungsmerkmal "Mobile Extension (MEX)" unterstützt, tragen Sie unter **MEX-Nummer** die vom ITSP zur Verfügung gestellte MEX-Nummer ein (8-stellig, nur Ziffern).

12) Zuordnung der Internet-Telefonie-Rufnummern - Möglichkeit 2:

Interne Nummer (Rufnr.) verwenden / Einzeleinträge: Sie haben einen Internet-Telefonie-Teilnehmeranschluss und als Internet-Telefonie-Rufnummern Einzelrufnummern erhalten (z. B. 70005555, 70005556,...). Diese Einzelrufnummern ordnen Sie anschließend den internen Rufnummern der Teilnehmer zu.



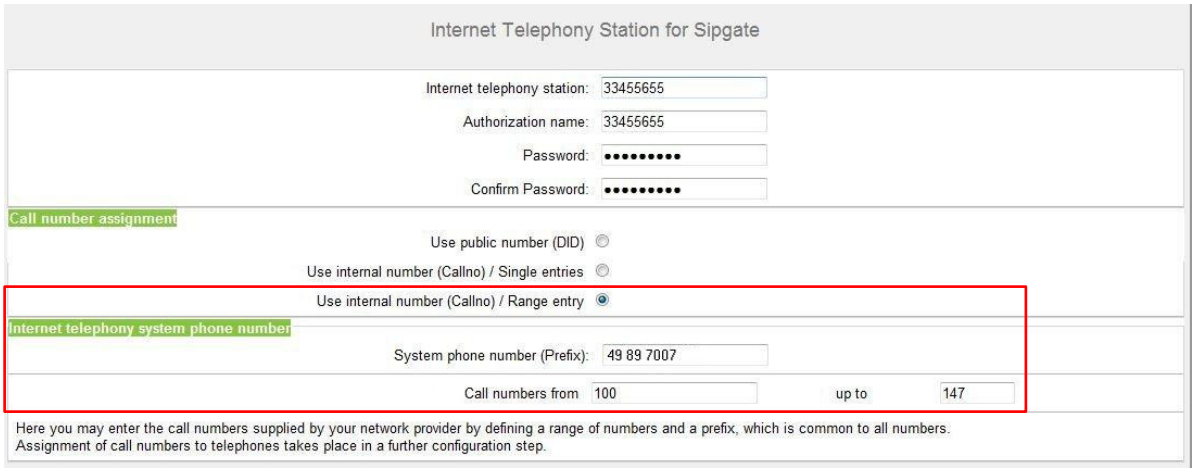
a) Wählen Sie im Bereich **Rufnummer assignment** das Optionsfeld **Interne Nummer (Rufnr.) verwenden / Einzeleinträge** aus.

b) Geben Sie im Bereich **Internet-Telefonie-Teilnehmerrufnummern** im Feld neben der Schaltfläche **Hinzufügen** eine der vom ITSP mitgeteilten Internet-Telefonie-Rufnummern ein und klicken Sie auf **Hinzufügen**.

c) Wenn Sie dem Account weitere Internet-Telefonie-Rufnummern zuordnen wollen, wiederholen Sie Schritt b).

13) Zuordnung der Internet-Telefonie-Rufnummern - Möglichkeit 3:

Interne Nummer (Rufnr.) verwenden / Bereichseintrag: Sie haben einen Internet-Telefonie-Anlagenanschluss und als Internet-Telefonie-Rufnummern ein Rufnummernband erhalten, z. B. (+49) 89 7007-100 bis (+49) 89 7007-147. Die Rufnummern aus dem Rufnummernband ordnen Sie anschließend den internen Rufnummern der Teilnehmer zu.



a) Wählen Sie im Bereich **Rufnummer assignment** das Optionsfeld **Interne Nummer (Rufnr.) verwenden / Bereichseintrag** aus.

b) Geben Sie unter **Anlagenrufnummer (Präfix)** die Anlagenrufnummer ein.

c) Geben Sie in den Feldern **Durchwahlband von** und **bis** das gewünschte Durchwahlband für den Internet-Telefonie-Teilnehmer ein. Standardmäßig ist 100 - 147 eingetragen.

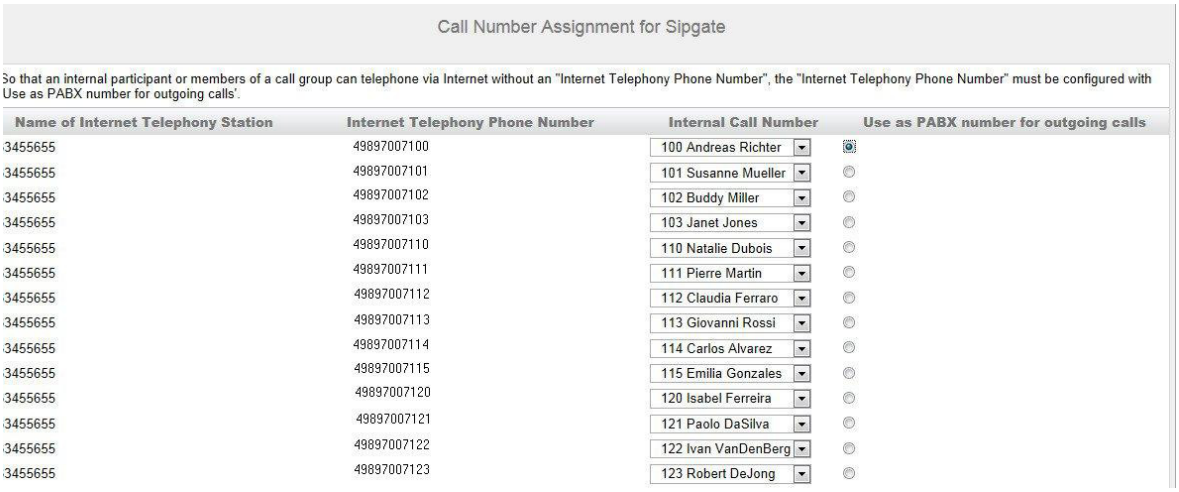
14) Klicken Sie auf **OK & Weiter**.

15) Wenn Sie weitere Accounts mit den dazugehörigen Internet-Telefonie-Rufnummern einrichten möchten, wiederholen Sie die Schritte 7 bis 14.

16) Klicken Sie auf **OK & Weiter**. Sie sehen eine Übersicht, welche Internet-Telefonie-Rufnummern welchen Accounts zugeordnet sind.

17) Ordnen Sie allen Internet-Telefonie-Rufnummern jeweils einer internen Rufnummer eines Teilnehmers zu.

Dieser Schritt entfällt, wenn Sie für die Zuordnung der Internet-Telefonie-Rufnummern die Möglichkeit 1 gewählt haben. Die Zuordnung treffen Sie in diesem Fall bei der Teilnehmer-Konfiguration im Feld **DuWa**.



a) Wählen Sie in der entsprechenden Zeile aus der Aufklappliste **interne Rufnummer** eine interne Rufnummer aus.

b) Sollen Teilnehmer ohne Internet-Telefonie-Rufnummer oder Mitglieder einer Rufgruppe externe Telefonate über das Internet führen dürfen, muss das Optionsfeld **Als gehende Anlagenrufnummer verwenden** aktiviert sein. Das Optionsfeld kann ausschließlich bei einer einzigen Internet-Telefonie-Rufnummer aktiviert sein.

18) Klicken Sie auf **OK & Weiter**. Hier sehen Sie nochmals die Liste der vordefinierten und neu hinzugefügten ITSP. Aktivierte ITSP sind in der Spalte **Provider aktivieren** mit einem Häkchen markiert. Mit **Restart ITSP** können Sie sich bei Verbindungsproblemen bei bereits aktivierten ITSP neu registrieren

19) Klicken Sie auf **OK & Weiter**.

20) Geben Sie im Feld **Upstream bis zu (Kbit/s)** den Wert der Upload-Geschwindigkeit Ihrer Internet-Verbindung ein. Nicht zu verwechseln mit der Download-Geschwindigkeit!

INFO: Im Feld **Anzahl simultaner Internet-Telefongespräche** wird Ihnen die Anzahl der gleichzeitig zu führenden Internet-Telefongespräche angezeigt. Wenn sich auf Grund der Netzauslastung die Gesprächsqualität verschlechtert, müssen Sie die Anzahl reduzieren.

---

21) Klicken Sie auf **OK & Weiter**.

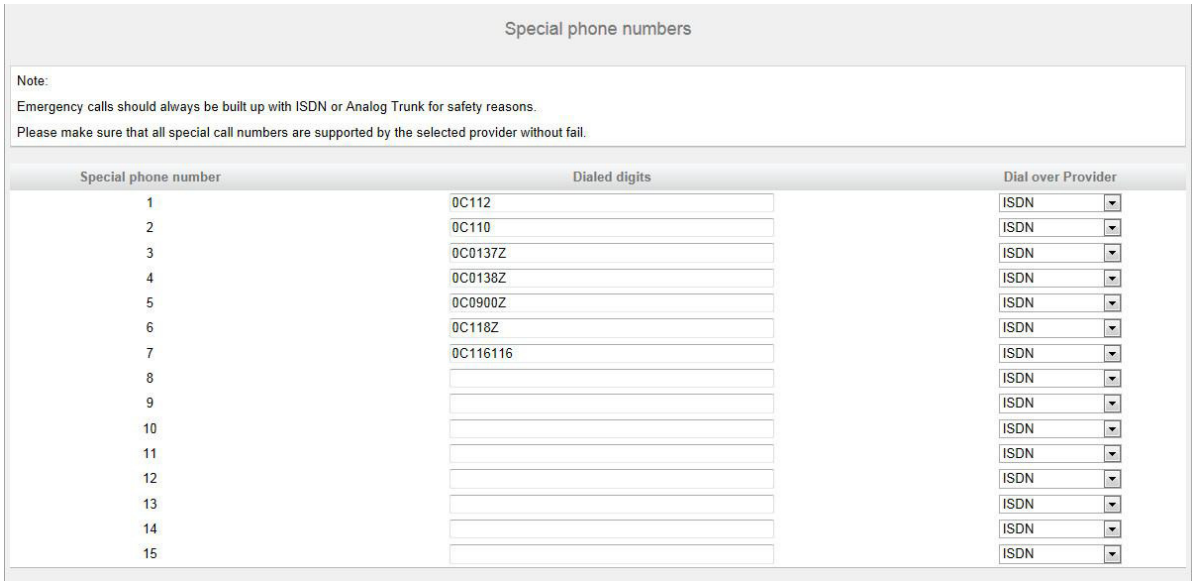
22) Falls Sie bei der Einrichtung Ihres Internet-Zugangs die Dauerverbindung noch nicht aktiviert haben, können Sie das hier nachholen. Ohne Dauerverbindung können Sie keine Anrufe über das Internet empfangen. Ist die Dauerverbindung bereits eingerichtet, erscheinen die unter a) bis c) beschriebenen Felder nicht.

a) Aktivieren Sie unter **Dauerverbindung** das Optionsfeld **An**.

b) Legen Sie im Feld **Zwangstrennung um (Std:Min)** die Uhrzeit fest, zu der die Internet-Verbindung getrennt werden soll (z. B. 04:59).

c) Klicken Sie auf **OK & Weiter**.

23) Tragen Sie in der Spalte **Gewählte Ziffern** die gewünschten Sonderrufnummern ein.



Folgende Rufnummerneinträge sind gültig:

0 bis 9: erlaubte Ziffern

-: Feldtrennzeichen

X: beliebige Ziffer zwischen 0 bis 9

N: beliebige Ziffer zwischen 2 bis 9

Z: eine oder mehrere Ziffern folgen bis Wahlende

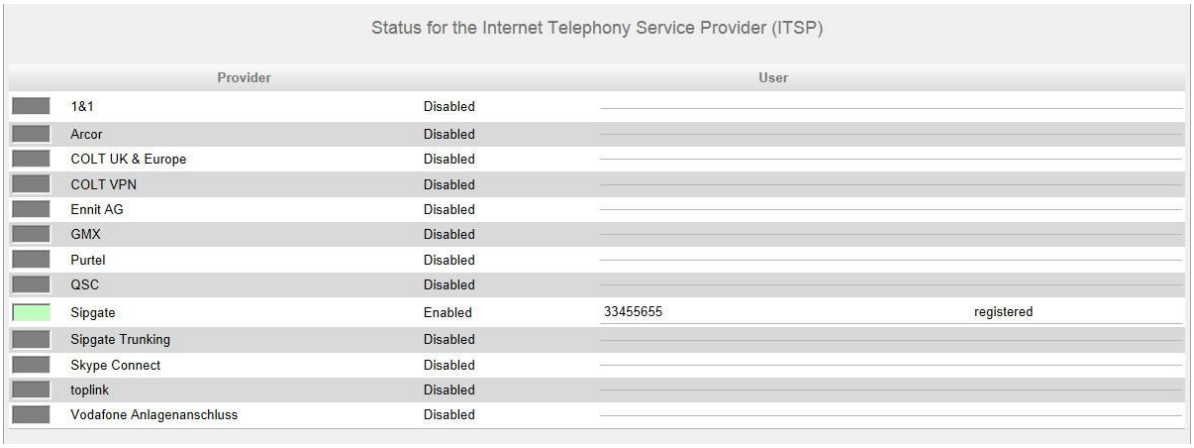
C: simulierter Wählton (kann max. 3 mal eingetragen werden)

24) Wählen Sie in der Spalte **Wählen über Provider** aus, ob die Sonderrufnummer über ISDN oder über einen ITSP gewählt werden soll. Es werden nur aktive ITSP angezeigt.

INFO: Stellen Sie sicher, dass Notrufnummern immer gewählt werden können. Falls Notrufnummern über einen Internet-Telefonie-Service-Provider gewählt werden sollen, muss der ITSP dies unterstützen.

---

25) Klicken Sie auf **OK & Weiter**. Es wird Ihnen der Status der ITSP angezeigt.



Grün markiert sind ITSP, die eingerichtet und an denen Sie bereits registriert sind.

Orange markiert sind ITSP, die eingerichtet und an denen Sie noch nicht registriert sind.

26) Klicken Sie auf **Weiter** und anschließend auf **Beenden**.

5.8.4.2 Wie Sie die Internet-Telefonie deaktivieren

Voraussetzungen

- Sie befinden sich im Fenster **Provider-Konfiguration und -Aktivierung für Internet-Telefonie**.

Schritt für Schritt

1) Lassen Sie das Kontrollkästchen **Keine Telefonie über Internet** aktiviert.

2) Klicken Sie zweimal auf **OK & Weiter**.

5.8.5 Teilnehmer

In den Fenstern **Teilnehmer auswählen - ...** konfigurieren Sie die an dem Kommunikationssystem angeschlossenen Teilnehmer.

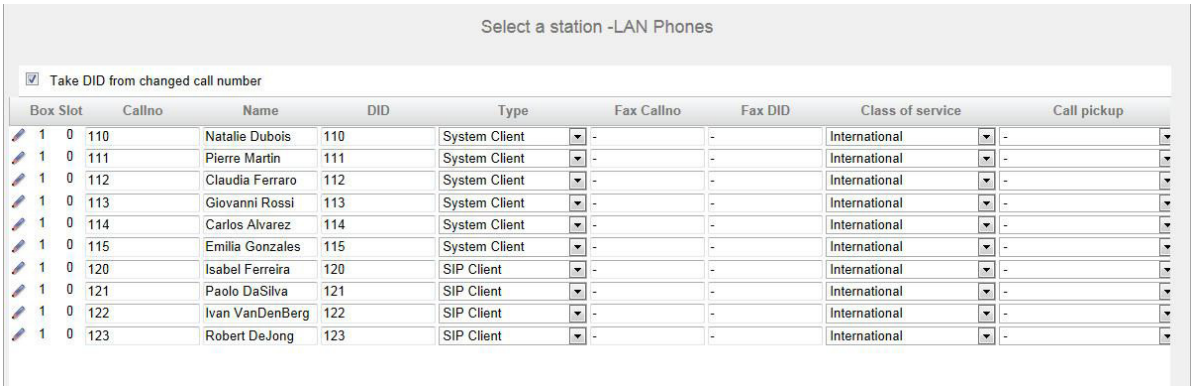
Gehen Sie folgendermaßen vor:

1. IP- und SIP-Teilnehmer konfigurieren
   IP-Teilnehmer und SIP-Teilnehmer sind z. B. LAN-Telefone oder WLAN-Telefone.

5.8.5.1 Wie Sie IP- und SIP-Teilnehmer konfigurieren

Voraussetzungen

- Sie befinden sich im Fenster **Teilnehmer auswählen - LAN-Telefone**.
- Für den Betrieb von WLAN-Telefonen benötigen Sie ein funktionsfähiges Wireless-LAN-Netzwerk.



Schritt für Schritt

1) Wenn sich die Durchwahlnummer des Teilnehmers von seiner Rufnummer unterscheiden soll, geben Sie in der Zeile des gewünschten Teilnehmers unter **DuWa** eine Durchwahl-Nummer für den Teilnehmer ein:

- nur bei Anlagenanschluss:

  Klicken Sie in das gewünschte Feld und geben Sie über die Tastatur die Durchwahlnummer ein. Die Durchwahlnummer kann auch mit der internen Rufnummer identisch sein.

- nur bei Mehrgeräteanschluss:

  Wählen Sie in dem gewünschten Feld über die Aufklappliste eine MSN aus. Der Teilnehmer kann z. B. von intern über die interne Rufnummer 101 und von extern über die MSN 654321 erreicht werden.

- bei Anlagenanschluss und Mehrgeräteanschluss:

  Wählen Sie in dem gewünschten Feld über die Aufklappliste den Eintrag **xxx - änderbar** aus (xxx steht für die interne Rufnummer) und geben Sie über die Tastatur die Durchwahlnummer ein oder wählen Sie über die Aufklappliste eine MSN aus.

2) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Rufnr** eine interne Rufnummer für den Teilnehmer ein. Sie können die vorbelegte Rufnummer verwenden oder eine andere, noch nicht belegte Rufnummer vergeben.

3) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Name** einen Namen in der Form `Nachname, Vorname` ein.

INFO: Der Name kann aus bis zu 16 Zeichen bestehen, sollte aber keine Umlaute oder Sonderzeichen enthalten. Der Name

wird wie hier angegeben bei den UC Clients als Nachname eingetragen, kann dort aber nachbearbeitet werden.

4) Wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Typ** den Typ des IP-Teilnehmers aus (z. B. "System Client" oder "SIP Client").

5) Wenn für den Teilnehmer eine Faxbox eingerichtet werden soll (nutzbar z. B. mit den UC Clients **myPortal for Desktop** oder **myPortal for Outlook**), gehen Sie folgendermaßen vor:

a) Geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax Rufnr** die gewünschte interne Fax-Rufnummer ein, unter der der Teilnehmer von intern Faxnachrichten empfangen kann.

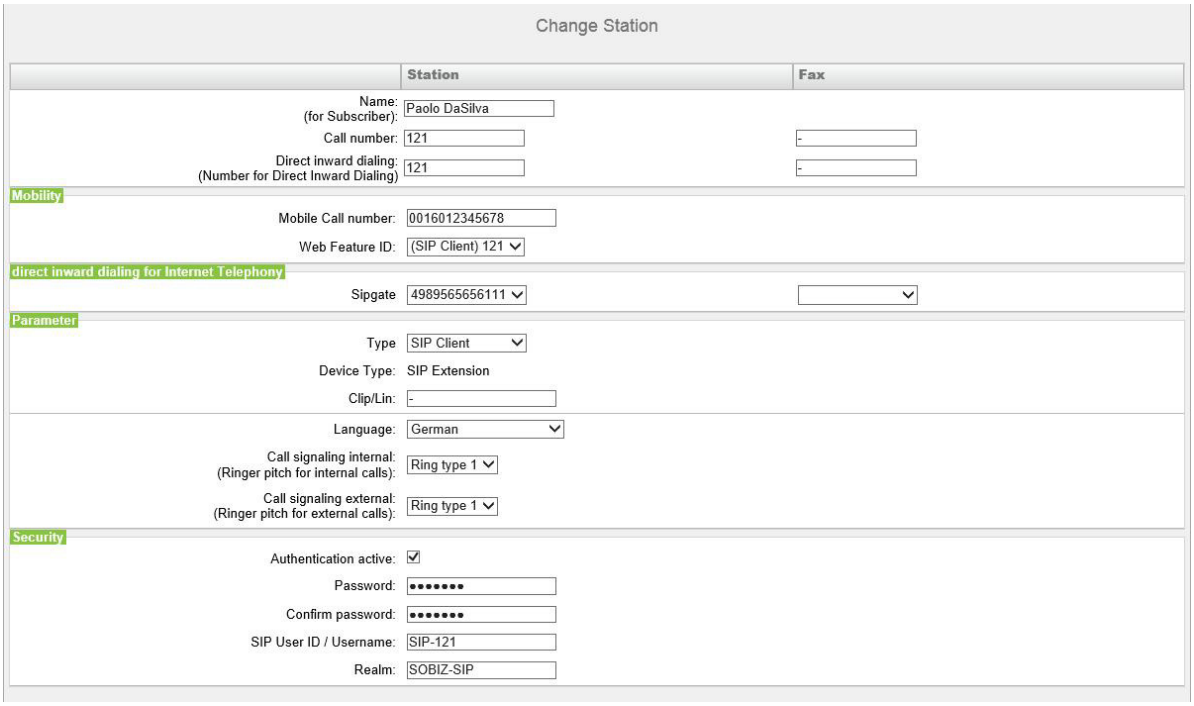
b) Wenn für die Faxbox eine Durchwahlnummer konfiguriert werden soll, geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax Durchwahl** die gewünschte externe Fax-Rufnummer ein, unter der der Teilnehmer von extern Faxnachrichten empfangen kann.

6) Wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Berechtigung** die gewünschte Berechtigungsgruppe aus.

7) Um den Teilnehmer in eine Anrufübernahmegruppe aufzunehmen, wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Anrufübernahme** eine Anrufübernahmegruppe aus.

8) Führen Sie die unter diesem Schritt beschriebenen Einstellungen nur bei Bedarf oder für ein SIP-Telefon durch:

a) Klicken Sie in der Zeile des gewünschten Teilnehmers auf das Stiftsymbol **Bearbeiten**.



b) Nur für SIP-Telefone: Wenn das SIP-Telefon zusammen mit einem Dual-Mode-Mobiltelefon betrieben werden soll, geben Sie im Bereich Mobility unter mobile Rufnummer die Amtskennziffer gefolgt von der Rufnummer des Mobiltelefons ein (z. B. 0016012345678). Wählen Sie zusätzlich aus der Aufklappliste Web Feature ID diesen SIP Client aus. (siehe *Dual-Mode-Telefonie*).

c) Geben Sie im Feld **Clip/Lin** eine Rufnummer ein (Durchwahlnummer oder MSN), die beim einem externen Anruf im Display des Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird.

INFO: Dieses Leistungsmerkmal muss vom Netzanbieter freigegeben sein.

---

d) Wählen Sie aus der Aufklappliste **Sprache** die Sprache für die Menüsteuerung des Telefons aus.

e) Weisen Sie aus der Aufklappliste **Rufsignalisierung intern** dem Teilnehmer eine von insgesamt acht möglichen akustischen Rufsignalisierungen für interne Anrufe zu. Dadurch sendet der Teilnehmer anderen internen Teilnehmern einen veränderten Rufton, durch den er von anderen Teilnehmern unterschieden werden kann (Standard: Rufart 1).

f) Weisen Sie aus der Aufklappliste **Rufsignalisierung extern** dem Teilnehmer eine von insgesamt drei möglichen akustischen Rufsignalisierungen für externe Anrufe zu (Standard: Rufart 1).

g) Nur für SIP-Telefone: Aktiveren Sie das Kontrollkästchen **Authentifizierung aktiv**.

h) Nur für SIP-Telefone: Geben Sie in den Feldern **Kennwort** und **Kennwort bestätigen** das Kennwort für die Authentifizierung ein.

i) Nur für SIP-Telefone: Geben Sie im Feld **SIP User ID / Benutzername** die Benutzerkennung für die Authentifizierung ein.

j) Nur für SIP-Telefone: Geben Sie im Feld **Realm** die zugehörige Zone für die Authentifizierung ein.

k) Klicken Sie auf **OK & Weiter**.

9) Wenn Sie einen weiteren IP-Teilnehmer einrichten möchten, klicken Sie auf **Daten speichern** und wiederholen Sie die Schritte 1 bis 8.

10) Klicken Sie auf **OK & Weiter**. Sie sehen eine Liste aller eingerichteten Teilnehmer. Diese Liste entspricht einem Rufnummernplan.

11) Klicken Sie bei Bedarf auf **Drucken**, um die Daten der eingerichteten Teilnehmer auszudrucken.

12) Klicken Sie anschließend auf **OK & Weiter**.

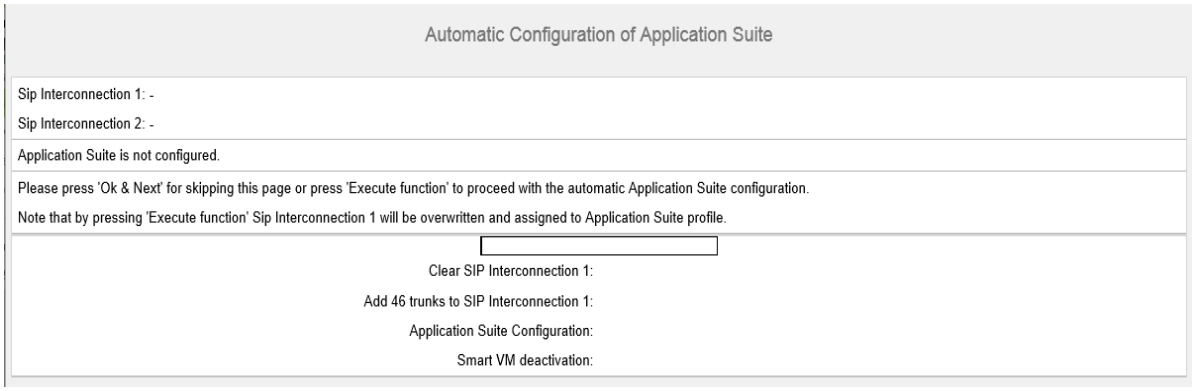
5.8.6 Konfiguration von UC Suite

Im Fenster **Automatische Konfiguration der Applikation-Suite** können Sie die automatische Konfiguration der UC-Lösung UC Suite durchführen.

5.8.6.1 Wie Sie UC Suite konfigurieren

Voraussetzungen

- Sie befinden sich im Fenster **Automatische Konfiguration der Application Suite**.



Schritt für Schritt

› Klicken Sie auf **Funktion ausführen**. Die UC Suite wird automatisch konfiguriert. Sobald der Verlaufsbalken 100% anzeigt, klicken Sie auf **OK & Weiter**.

5.8.7 Konferenz-Server-Einstellungen (nur mit UC Suite)

Im Fenster **MeetMe-Konferenz-Einstellungen ändern** können Sie die Rufnummer und die Einwahlnummer für Konferenzen festlegen.

INFO: Dieses Fenster erscheint nur, wenn im Wizard **Erstinstallation** bei der Applikationsauswahl **Paket mit UC Suite ...** gewählt wurde.

5.8.7.1 Wie Sie die Konferenz-Server-Einstellungen ändern

Voraussetzungen

- Die Hard- und Software für die Nutzung von UC Suite ist vorhanden.
- Sie befinden sich im Fenster **MeetMe-Konferenz-Einstellungen ändern**.



Schritt für Schritt

1) Geben Sie im Feld **Rufnummer** eine Rufnummer für die Konferenz ein.
2) Legen Sie im Feld **Durchwahl** die Einwahlnummer für die Konferenz (Konferenz-DUWA) fest, mit der sich Teilnehmer in eine bestehende Konferenz einwählen können.
3) Klicken Sie auf **OK & Weiter**.

5.8.8 E-Mail-Versand (optional)

Im Fenster **E-Mail-Weiterleitung ändern** können Sie den E-Mail-Versand konfigurieren. Teilnehmer werden dadurch über neue Sprach- und Faxnachrichten informiert und der Administrator erhält Systemmeldungen.

Sie haben folgende Möglichkeiten:

- E-Mail-Versand konfigurieren
  Sie können einen externen E-Mail-Server festlegen, über den OpenScape Business die E-Mails versenden soll. Sprach- und Faxnachrichten oder interne Systemmeldungen werden über diesen E-Mail-Server an eine oder verschiedene konfigurierbare E-Mail-Adressen versendet.

> ***INFO:*** Die Angabe eines E-Mail-Servers ist wichtig, wenn den Benutzern der UC Suite automatisch per E-Mail ein Link auf die Installationsdatei(en) geschickt werden soll.

5.8.8.1 Wie Sie den E-Mail-Versand konfigurieren

Voraussetzungen

- Es ist ein E-Mail-Konto mit einem Kennwort bei einem E-Mail-Provider vorhanden und Sie kennen die Zugangsdaten.
- Sie befinden Sich im Fenster **E-Mail-Weiterleitung ändern**.



Schritt für Schritt

1) Geben Sie den **Postausgangs-Server (SMTP)** für den E-Mail-Server ein, der für den E-Mail-Versand genutzt werden soll, z. B. `smtp.web.de`. Erfragen Sie den Postausgangs-Server ggf. bei Ihrem E-Mail-Provider.

> ***INFO:*** Achten Sie darauf, dass der Name des Postausgangs-Servers aufgelöst werden kann. Falls nicht, müssen Sie den Wizard für den E-Mail-Versand starten über **Service-Center > Email-Weiterleitung** und anstelle des Namens des Postausgangs-Servers die IP-Adresse des Postausgangs-Servers eingeben.

2) Wenn eine sichere Verbindung erforderlich ist, aktivieren Sie das Kontrollkästchen. Erfragen Sie ggf. bei Ihrem E-Mail-Provider, ob diese Option aktiviert werden muss.

3) Geben Sie den **Benutzernamen** des E-Mail-Kontos ein z. B. `max.mustermann`.

4) Geben Sie unter **Kennwort** und **Kennwort wiederholen** das Kennwort des E-Mail-Kontos ein.

5) Geben Sie die **E-Mail-Adresse** ein, z. B. `max.mustermann@web.de`.

6) Wenn Sie die eingegebenen E-Mail-Einstellungen sofort testen wollen, gehen Sie folgendermaßen vor:

a) Klicken Sie auf **Weiterleitung testen**.

b) Geben Sie unter **Senden an E-Mail-Adresse** die E-Mail-Adresse eines E-Mail-Postfachs ein, auf das Sie Zugriff haben. An diese E-Mail-Adresse wird die Test-E-Mail geschickt.

c) Geben Sie unter **Betreff in der Email** einen beschreibenden Text ein, um die E-Mail in Ihrem E-Mail-Postfach identifizieren zu können.

d) Klicken Sie auf **Testmail senden**. Die E-Mail-Einstellungen werden überprüft und die E-Mail an das angegebene E-Mail-Postfach abgeschickt.

e) Überprüfen Sie, ob die E-Mail in Ihrem E-Mail-Postfach angekommen ist.

f) War der E-Mail-Versand erfolgreich, gehen Sie zum nächsten Schritt.

g) War der E-Mail-Versand nicht erfolgreich, klicken Sie auf **Zurück** und überprüfen nochmal Ihre E-Mail-Einstellungen.

7) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**. Die Basisinstallation ist beendet. Bevor Sie die im Wizard erwähnte Datensicherung durchführen, sollten Sie die Lizenzen aktivieren.

5.9 Abschließende Tätigkeiten

Nachdem die Erstinstallation und die Basisinstallation mit dem WBM abgeschlossen sind, müssen noch einige wichtige Einstellungen für den Betrieb von OpenScape Business getroffen werden.

Gehen Sie folgendermaßen vor:

1. Remote Service SSDP einschalten
   Sie können den autorisierten Servicetechnikern eines Remote Service Partners über die internetbasierte Plattform für Remote Services (SSDP, Smart Services Delivery Platform) den Zugriff auf das Kommunikationssystem ermöglichen. Damit ist z. B. die Unterstützung bei der Lösung von Administrationsaufgaben oder bei der Fehlersuche möglich.Jeder Remote Service Partner, der SSDP nutzt, hat eine eigene Partner ID. Mit der vorbelegten Partner ID "Unify" kann der Fernzugriff durch autorisiertes Servicepersonal des Herstellers aktiviert werden.
   Für die Konfiguration von SSDP siehe *Remote Services*
2. Lizenzen aktivieren und zuordnen
   Die mit OpenScape Business erworbenen Lizenzen müssen innerhalb einer Zeitspanne von 30 Tagen aktiviert werden. Die Zeitspanne startet beim ersten Anmelden am WBM. Nach Ablauf der Zeitspanne ist das Kommunikationssystem nur noch eingeschränkt nutzbar. Nach erfolgreicher Aktivierung müssen die Lizenzen den Teilnehmern und Leitungen zugeordnet werden. Systemweite Leistungsmerkmale sind bereits mit der Aktivierung freigeschaltet.
3. UC Clients zur Installation bereitstellen
   Die UC Clients sind Bestandteil der UC Suite. Die Installationsdateien für die UC Clients sind über das WBM zugänglich und können den IP-Teilnehmern automatisch oder manuell zur Verfügung gestellt werden.
   Zusätzlich gibt es für den Administrator die Möglichkeit der Silent Installation. Dabei handelt es sich um eine kommandozeilenbasierte Methode zur automatischen Installation, Deinstallation und Modifikation von UC Suite Clients auf einem PC ohne weitere erforderliche Eingaben. Für weitere Informationen siehe *Silent Installation/Deinstallation für UC Suite PC-Clients*.
4. Datensicherung durchführen
   Die bisherigen Änderungen an OpenScape Business müssen gesichert werden. Die Sicherung kann als Backup-Set z. B. im internen Netz gespeichert werden.

5.9.1 Wie Sie den Remote Service SSDP einschalten

Voraussetzungen

- Ein Internet-Zugang und eine funktionierende DNS-Konfiguration liegen vor.
- Die Partner ID Ihres Remote Service Partners liegt vor (vorbelegte Partner ID: Unify)
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Remote-Zugang**.

3) Klicken Sie auf **Aktivierung / Deaktivierung**, um den Wizard **Aktivierung / Deaktivierung des Service-Plugin** zu starten.

4) Ändern Sie im Feld **Partner ID** bei Bedarf die vorbelegte Partner ID und klicken Sie auf **Sichern**.

5) Klicken Sie auf **Aktivieren**.

5.9.2 Wie Sie die Lizenzen aktivieren und zuordnen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.
- Sie kennen den LAC (Lizenz-Autorisierungscode) für die Lizenzfreischaltung und haben eine Benutzerkennung und ein Passwort für den Zugang zum Lizenzserver.
- Für die Verbindung zum Lizenzserver ist ein Internet-Zugang nötig.

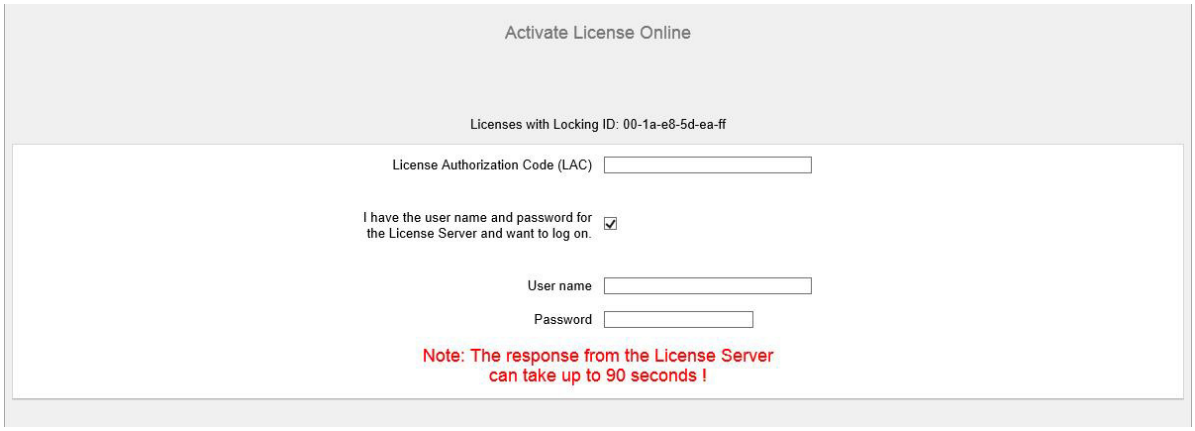
Schritt für Schritt

1) Lizenzen online aktivieren:

a) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

b) Klicken Sie im Navigationsbaum auf **Wizards > Grundinstallation**.

c) Klicken Sie auf **Bearbeiten**, um den Wizard **Lizenzierung** zu starten.



d) Geben Sie im Feld **Lizenz Autorisierungs Code (LAC)** den LAC ein.

e) Aktivieren Sie das Kontrollkästchen **Ich habe Benutzernamen und Kennwort für den Lizenzserver und möchte mich anmelden**.

f) Geben Sie **Benutzername** und **Kennwort** für die Anmeldung am Lizenzserver ein.

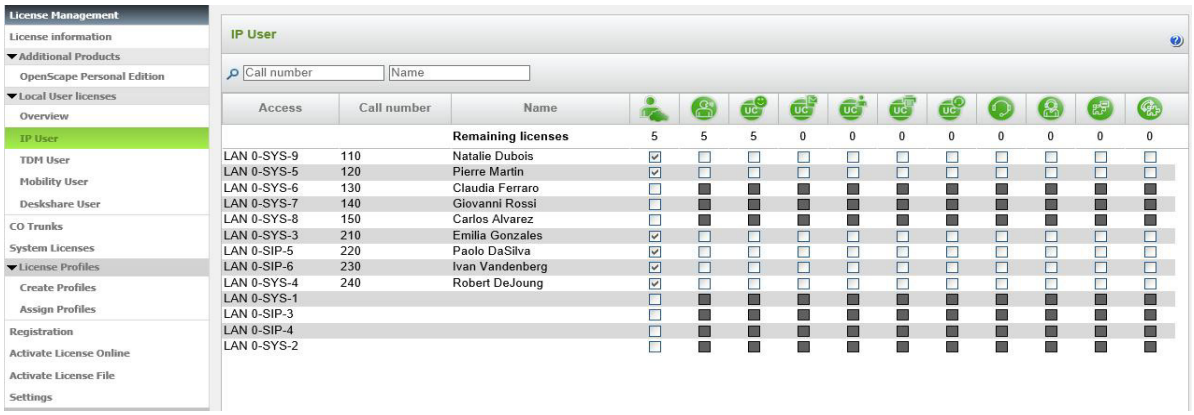
g) Klicken Sie auf **OK & Weiter**. Die Verbindung zum Lizenzserver wird hergestellt und die Lizenzen freigeschaltet.

2) Lizenzen den Teilnehmern zuordnen:

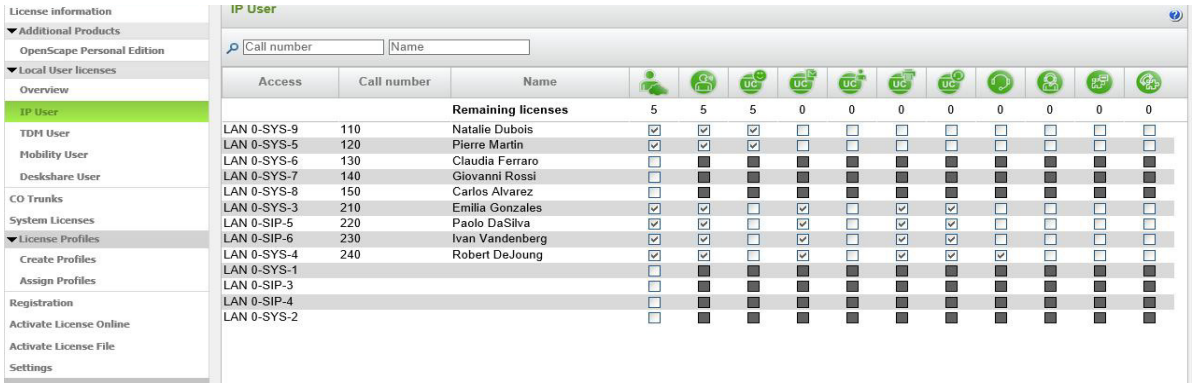
a) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.

b) Navigieren Sie im Navigationsbaum auf **Lokale Benutzerlizenzen > ...** zum gewünschten Teilnehmer-Typ. Es wird Ihnen eine Liste aller Teilnehmer des ausgewählten Teilnehmer-Typs angezeigt.

c) Aktivieren Sie in der Zeile des gewünschten Teilnehmers das Kontrollkästchen in der Spalte **Benutzer-Lizenz** (erste Spalte mit Kontrollkästchen).



d) Aktivieren Sie in der Zeile des gewünschten Teilnehmers die User-orientierten Lizenzen, indem Sie die gewünschten Kontrollkästchen aktivieren.



INFO: User-orientierte Lizenzen können einem Teilnehmer nur zugewiesen werden, wenn dem Teilnehmer zuvor eine Teilnehmer-Lizenz (Benutzer-Lizenz) zugeordnet wurde (Schritt c).

e) Klicken Sie auf **OK & Weiter**. Es wird geprüft, ob für Ihre Zuordnung genügend Lizenzen vorhanden sind.

Sind ausreichend Lizenzen vorhanden ist die Lizenzierung der Teilnehmer beendet.

f) Fehlen Lizenzen, werden Ihnen die Fehler mit einem rot hinterlegten Kontrollkästchen angezeigt. Korrigieren Sie diese Fehler und wiederholen Sie Schritt e.

3) Lizenzen den Leitungen zuordnen:

a) Klicken Sie im Navigationsbaum auf **Amtsleitungen**. Im Bereich **Amtsleitungen** wird Ihnen die Anzahl der erworbenen Leitungslizenzen angezeigt.

b) Für SIP-Leitungen: Geben Sie im Bereich **Bedarf an Lizenzen für gleichzeitige Internet-Anrufe in diesem Knoten** die Anzahl der Internet-Gespräche an, die gleichzeitig über einen ITSP geführt werden können.

c) Klicken Sie auf **OK & Weiter**.

5.9.3 Wie Sie die UC Suite Clients zur Installation bereitstellen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.
- Die Hard- und Software für die Nutzung von UC Suite ist vorhanden.

INFO: Für die Nutzung der UC Suite Clients sind Lizenzen nötig.

Schritt für Schritt

1) Damit die Installationsdateien einem Teilnehmer automatisch zur Verfügung gestellt werden können, vergewissern Sie sich, ob folgende Schritte durchgeführt worden sind:

a) Die E-Mail-Adressen der Teilnehmer müssen entweder zusammen mit den Teilnehmerdaten über eine XML-Datei importiert worden sein oder eingetragen werden unter **Einrichtung > UC Suite > Benutzerverzeichnis**.

b) Ein Mail-Server muss eingetragen sein.

INFO: Einen E-Mail-Server können Sie auch nachträglich eintragen unter **Service-Center > Email-Weiterleitung**.

Alle Teilnehmer, deren E-Mail-Adressen bekannt sind, erhalten eine E-Mail mit dem Link auf das Installationsverzeichnis der UC Clients und mit einer Erste-Schritte-Anleitung. Im Installationsverzeichnis liegt zusätzlich eine Readme-Datei mit Informationen zur Installation der Software auf den Client-PCs.

2) Falls die nötigen Schritte für eine automatische Benachrichtigung nicht erfüllt sind, können Sie die Installationsdateien auch manuell zur Verfügung stellen. Gehen Sie dazu folgendermaßen vor:

a) Klicken Sie in der Navigationsleiste auf **Service-Center**.

b) Klicken Sie im Navigationsbaum auf **Software**.

c) Klicken Sie auf den gewünschten UC Client und speichern Sie die gezippte Installationsdatei auf einem freigegebenen Netz-Laufwerk.

d) Klicken Sie im Navigationsbaum auf **Dokumente** und wählen Sie die Aufklappliste **Bedienungsanleitung**.

e) Klicken Sie auf die Dokumentation zum gewünschten UC Client und speichern Sie die Dokumentationsdatei auf einem freigegebenen Netz-Laufwerk.

f) Senden Sie den Benutzern der UC Clients die gezippte Installationsdatei und die Dokumentationsdatei per E-Mail oder teilen Sie den Benutzern den Ablageort der Dateien mit.

g) In der Zip-Datei mit den Installationsdateien ist auch eine Readme-Datei enthalten. Weisen Sie die Benutzer darauf hin, dass die Installation der UC Clients anhand der Installationshinweise in der Readme-Datei durchgeführt werden muss.

3) Alternativ können Sie den UC Benutzern auch Links zuschicken, über die sie direkt auf die Installationsdateien der UC Clients zugreifen können.

a) Klicken Sie in der Navigationsleiste auf **Service-Center**.

b) Klicken Sie im Navigationsbaum auf **Software**.

c) Klicken Sie auf die Schaltfläche **Applikationslinks anzeigen**. Es werden Ihnen mehrere Links angezeigt, abhängig vom verwendeten Betriebssystem und vom gewünschten UC Client, z. B.:

```
https://<IP-Adresse des Kommunikationssystems>/
management/downloads/install-common.zip
```

5.9.4 Wie Sie die Datensicherung durchführen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

INFO: Weitere Informationen zur Datensicherung siehe *Sofortiges Sichern*.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Datensicherung**.

2) Klicken Sie im Navigationsbaum auf **Backup - sofort**.

3) Geben Sie im Bereich **Name** im Feld **Kommentar** einen Kommentar für das Backup-Set ein, um das Backup-Set bei einer möglichen Wiederherstellung leichter identifizieren zu können. Vermeiden Sie bei der Eingabe Umlaute und Sonderzeichen.

4) Aktivieren Sie im Bereich **Geräte** das Ziellaufwerk, auf dem das Backup-Set gespeichert werden soll (z B. auf einem Netzlaufwerk).

5) Klicken Sie auf **OK & Weiter**. In einem weiteren Fenster wird Ihnen der Fortschritt der Sicherung angezeigt.

6) Die Sicherung ist erfolgreich, wenn die Meldung **Sicherung erfolgreich ausgeführt!** erscheint. Klicken Sie auf **Beenden**.

7) Die Erstinbetriebnahme mit dem WBM ist nun abgeschlossen. Beenden Sie das WBM, indem Sie rechts oben auf den Link **Abmelden** klicken und anschließend das Fenster schließen.

5.10 Inbetriebnahme der IP-Telefone

Eine komfortable Inbetriebnahme der IP-Telefone erfordert einen DHCP-Server, der das IP-Telefon mit den für die Anmeldung am Kommunikationssystem wichtigen Daten (netzwerkspezifische Daten) versorgt.

Netzwerkspezifische Daten

Ein IP-Telefon benötigt für die Anmeldung am Kommunikationssystem netzwerkspezifische Daten. Diese Daten können einerseits im DHCP-Server gespeichert sein oder direkt am IP-Telefon eingegeben werden. Vorteil eines DHCP-Servers

ist, dass alle angeschlossenen IP-Telefone automatisch mit den Daten versorgt werden.

Folgende Daten werden vom IP-Telefon benötigt:

- IP-Adresse des Kommunikationssystems
- IP-Adresse des DLS-Servers

Zusätzlich benötigt das IP-Telefon noch die eigene Rufnummer. Diese muss während der Anmeldung manuell am Telefon eingetragen werden.

Registrierung von SIP-Telefonen

Aus Sicherheitsgründen ist es empfehlenswert, dass sich SIP-Telefone am Kommunikationssystem registrieren. Dazu müssen die Registrationsdaten am IP-Telefon und im Kommunikationssystem übereinstimmen.

Folgende Daten werden für die Anmeldung benötigt:

- SIP-Benutzer-ID
- SIP-Passwort
- SIP-Realm (optional)

Verwenden Sie ein nicht triviales SIP-Passwort, das folgende Regeln erfüllt:

- Mindestens 8 Stellen
- Mindestens einen Großbuchstaben (A - Z)
- Mindestens einen Kleinbuchstaben (a - z)
- Mindestens eine Ziffer (0-9)
- Mindestens ein Sonderzeichen

Verwenden Sie eine SIP-Benutzer-ID, die nicht die Telefonnummer enthält.

INFO: Weitere Informationen zur Einrichtung von SIP-Telefonen finden Sie unter `http://wiki.unify.com/wiki/SIP_devices_configuration_examples`.

Nutzung des internen DHCP-Servers

Wird der interne DHCP-Server des Kommunikationssystems genutzt, sind die netzwerkspezifischen Daten dort bereits hinterlegt. Damit sich ein IP-Telefon am Kommunikationssystem registrieren kann, muss am IP-Telefon nur die festgelegte Rufnummer eintragen werden. Für ein SIP-Telefon müssen zusätzlich die Daten zur SIP-Registrierung am SIP-Telefon und am Kommunikationssystem übereinstimmen.

Nutzung eines externen DHCP-Servers mit netzwerkspezifischen Daten

Wird ein externer DHCP-Server genutzt, sind die netzwerkspezifischen Daten dort zu hinterlegen. Damit sich ein IP-Telefon am Kommunikationssystem registrieren kann, muss am IP-Telefon nur die festgelegte Rufnummer eintragen werden. Für ein SIP-Telefon müssen zusätzlich die Daten zur SIP-Registrierung am SIP-Telefon und am Kommunikationssystem übereinstimmen.

Nutzung eines externen DHCP-Servers ohne netzwerkspezifische Daten

Wird ein externer DHCP-Server genutzt, bei dem die netzwerkspezifischen Daten nicht hinterlegt werden können, müssen diese am IP-Telefon eingegeben werden. Damit sich ein IP-Telefon am Kommunikationssystem registrieren kann, müssen am IP-Telefon die festgelegte Rufnummer und die IP-Adresse des Kommunikationssystems eintragen und evtl. die Einstellungen für den Deployment Service geändert werden. Für ein SIP-Telefon müssen zusätzlich die Daten zur SIP-Registrierung am SIP-Telefon und am Kommunikationssystem übereinstimmen.

5.10.1 Wie Sie ein IP-Telefon konfigurieren

Voraussetzungen

- Das IP-Telefon ist an das interne Netz angeschlossen und betriebsbereit.

> ***INFO:*** Hier wird die Konfiguration am Beispiel eines OpenStage 40/60/80 IP-Systemtelefons beschrieben. Für ein anderes IP-Telefon müssen diese Einstellungen analog durchgeführt werden. Sehen Sie dazu bitte in der Anleitung Ihres IP-Telefons nach.

Schritt für Schritt

1) Um in den Administrationsmodus des IP-Systemtelefons zu gelangen, drücken Sie am Telefon die Taste für das Einstellungen-/Anwendungen-Menü.

2) Blättern Sie im Register `Einstellungen` bis `Admin` und bestätigen Sie mit der OK-Taste.

3) Geben Sie das Administrator-Passwort (Standard: `123456`) ein und bestätigen Sie mit der OK-Taste.

4) Wenn Sie im internen Netz den DHCP-Server des Kommunikationssystems verwenden, überspringen Sie den nächsten Schritt.

5) Wenn Sie im internen Netz nicht den DHCP-Server des Kommunikationssystems verwenden, müssen Sie die IP-Adresse des Deployment Servers (DLS) und des Kommunikationssystems eingeben, damit die Software des IP-Systemtelefons automatisch aktualisiert werden kann. Das gilt nur für IP-Systemtelefone. Führen Sie dazu folgende Schritte durch:

- ***a)*** Blättern Sie bis `Network` und bestätigen Sie mit der OK-Taste.
- ***b)*** Blättern Sie bis `Update service (DLS)` und bestätigen Sie mit der OK-Taste.
- ***c)*** Blättern Sie bis `DLS address` und bestätigen Sie mit der OK-Taste.
- ***d)*** Geben Sie als Deployment Server die IP-Adresse des Kommunikationssystems (Standard: `192.168.1.2`) an und bestätigen Sie mit der OK-Taste.

e) Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.

f) Blättern Sie bis `IPv4 configuration` und bestätigen Sie mit der OK-Taste.

g) Blättern Sie bis `Route (default)` und bestätigen Sie mit der OK-Taste.

h) Geben Sie die IP-Adresse des Kommunikationssystems (Standard: `192.168.1.2`) an und bestätigen Sie mit der OK-Taste.

i) Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.

j) Navigieren Sie eine Menüebene zurück mit der Zurück-Taste.

6) Legen Sie die Rufnummer des Telefons fest:

a) Blättern Sie bis `System` und bestätigen Sie mit der OK-Taste.

b) Blättern Sie bis `Identity` und bestätigen Sie mit der OK-Taste.

c) Blättern Sie bis `Terminal number` und bestätigen Sie mit der OK-Taste.

d) Geben Sie die festgelegte Rufnummer ein (z. B. `120`) und bestätigen Sie mit der OK-Taste.

e) Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.

7) Navigieren Sie eine Menüebene zurück mit der Zurück-Taste.

8) Wenn das Systemtelefon bedingt durch die Änderungen einen Neustart durchführen muss, erscheint in dem Menü `Admin` der Menüpunkt `Restart`. Bestätigen Sie `Restart` mit der OK-Taste und anschließend `Yes` ebenso mit der OK-Taste. Das Systemtelefon führt einen Neustart durch und meldet sich am Kommunikationssystem an.

5.10.2 Wie Sie ein SIP-Telefon konfigurieren

Voraussetzungen

- Das SIP-Telefon ist an das Kunden-LAN angeschlossen und betriebsbereit.

> ***INFO:*** Hier wird die Konfiguration am Beispiel eines OpenStage 40/60/80 SIP-Systemtelefons beschrieben. Für ein anderes SIP-Telefon müssen diese Einstellungen analog durchgeführt werden. Sehen Sie dazu bitte in der Anleitung Ihres SIP-Telefons nach.

Schritt für Schritt

1) Um in den Administrationsmodus des SIP-Systemtelefons zu gelangen, drücken Sie am Telefon die Taste für das Einstellungen-/Anwendungen-Menü.

2) Blättern Sie im Register `Einstellungen` bis `Administrator (Admin)` und bestätigen Sie mit der OK-Taste.

3) Geben Sie das Administrator-Passwort (Standard: `123456`) ein und bestätigen Sie mit der OK-Taste.

4) Wenn Sie im internen Netz den DHCP-Server des Kommunikationssystems verwenden, überspringen Sie den nächsten Schritt.

5) Wenn Sie im internen Netz nicht den DHCP-Server des Kommunikationssystems verwenden, müssen Sie die IP-Adresse des Deployment Servers (DLS) und des Kommunikationssystems eingeben, damit die Software des SIP-Systemtelefons automatisch aktualisiert werden kann. Das gilt nur für SIP-Systemtelefone. Führen Sie dazu folgende Schritte durch:

- ***a)*** Blättern Sie bis `Network` und bestätigen Sie mit der OK-Taste.
- ***b)*** Blättern Sie bis `Update service (DLS)` und bestätigen Sie mit der OK-Taste.
- ***c)*** Blättern Sie bis `DLS address` und bestätigen Sie mit der OK-Taste.
- ***d)*** Geben Sie als Deployment Server die IP-Adresse des Kommunikationssystems (Standard: `192.168.1.2`) an und bestätigen Sie mit der OK-Taste.
- ***e)*** Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.
- ***f)*** Blättern Sie bis `IPv4 configuration` und bestätigen Sie mit der OK-Taste.
- ***g)*** Blättern Sie bis `Route (default)` und bestätigen Sie mit der OK-Taste.
- ***h)*** Geben Sie die IP-Adresse des Kommunikationssystems (Standard: `192.168.1.2`) an und bestätigen Sie mit der OK-Taste.
- ***i)*** Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.
- ***j)*** Navigieren Sie eine Menüebene zurück mit der Zurück-Taste.

6) Legen Sie die SNTP-Zeiteinstellungen fest:

- ***a)*** Blättern Sie bis `Date and time` und bestätigen Sie mit der OK-Taste.
- ***b)*** Blättern Sie bis `Time source` und bestätigen Sie mit der OK-Taste.
- ***c)*** Blättern Sie bis `SNTP IP address` und bestätigen Sie mit der OK-Taste.
- ***d)*** Geben Sie die IP-Adresse des Kommunikationssystems (Standard: `192.168.1.2`) an und bestätigen Sie mit der OK-Taste.
- ***e)*** Blättern Sie bis `Timezone offset` und bestätigen Sie mit der OK-Taste.
- ***f)*** Geben Sie die Abweichung der lokalen Uhrzeit von der UTC-Zeit (Universal Time Coordinated) in Stunden an (Deutschland: `1`) und bestätigen Sie mit der OK-Taste.
- ***g)*** Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.
- ***h)*** Navigieren Sie eine Menüebene zurück mit der Zurück-Taste.

7) Legen Sie die Rufnummer des Telefons fest:

- ***a)*** Blättern Sie bis `System` und bestätigen Sie mit der OK-Taste.
- ***b)*** Blättern Sie bis `Identity` und bestätigen Sie mit der OK-Taste.
- ***c)*** Blättern Sie bis `Terminal number` und bestätigen Sie mit der OK-Taste.

d) Geben Sie die festgelegte Rufnummer ein (z. B. `120`) und bestätigen Sie mit der OK-Taste.

e) Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.

8) Legen Sie die SIP-Authentifizierungsdaten fest:

a) Blättern Sie bis `Registration` und bestätigen Sie mit der OK-Taste.

b) Blättern Sie bis `SIP session` und bestätigen Sie mit der OK-Taste.

c) Notieren Sie sich die `Realm` oder geben Sie bei Bedarf eine neue Realm (z. B. `OSBIZ-SIP`) ein.

d) Notieren Sie sich die `User ID` oder geben Sie bei Bedarf eine neue User ID (z. B. `SIP-120`) ein.

e) Vergeben Sie ein `Passwort` für die Registrierung am SIP Server.

f) Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.

9) Navigieren Sie mit der Zurück-Taste zum Menü `Admin` zurück.

10) Wenn das Systemtelefon bedingt durch die Änderungen einen Neustart durchführen muss, erscheint in dem Menü `Admin` der Menüpunkt `Restart`. Bestätigen Sie `Restart` mit der OK-Taste und anschließend `Yes` ebenso mit der OK-Taste. Das Systemtelefon führt einen Neustart durch und meldet sich am Kommunikationssystem an.

5.11 Deinstallation der Kommunikationssoftware

Die Deinstallation der Kommunikationssoftware ist über eine Text-Konsole möglich.

5.11.1 Wie Sie die Kommunikationssoftware deinstallieren

Schritt für Schritt

1) Öffnen Sie ein Terminal (z. B. GNOME Terminal).

2) Geben Sie in der Shell-Oberfläche den Befehl `su` (für superuser = root) ein und bestätigen Sie mit der Eingabetaste.

3) Geben Sie in der Shell-Oberfläche das Passwort für den Benutzer "root" ein und bestätigen Sie mit der Eingabetaste.

4) Geben Sie in der Shell-Oberfläche den Befehl `oso_deinstall.sh` ein und bestätigen Sie mit der Eingabetaste. Folgen Sie den Anweisungen des Deinstallationsprogramms.

5.12 Verwendete Ports

Die OpenScape Business Systemkomponenten nutzen verschiedene Ports, die bei Bedarf in der Firewall freigeschaltet werden müssen. Für die Ports der

Webbased Clients (z. B. myPortal to go) muss ein Port Forwarding im Router eingerichtet werden.

INFO: Die in der u.a. Liste mit "O" gekennzeichneten Ports sind optional, d.h. sie sind nicht dauerhaft in der Firewall geöffnet (z. B. ist der TFTP-Port nur bei aktiviertem Gate View offen).

Beschreibung	TCP	UDP	Portnummer	OpenScape Business X	UC Booster Card	OpenScape Business S	UC Booster Server
Systemkomponenten							
Admin Portal (https)	X		443	X	X	X	X
CAR Update Registration	X		12061	X		X	
CAR Update Server	X		12063	X		X	
CLA	X		61740	O		O	O
CLA Auto Discovery		X	23232	X		X	X
CSTA Message Dispatcher (CMD)	X		8900		X	X	X
CSTA Protocol Handler (CPH)	X		7004	X		X	
CSTA Service Provider (CSP)	X		8800		X	X	X
DHCP		X	67	X			
DLI	X		18443	X		X	X
DLSC	X		8084	X		X	X
DNS	X	X	53	X			
FTP	X		21	O		O	
FTP Passive	X		40000:40040	O		O	
Gate View	X		8000:8010		O	O	O
HFA	X		4060	X		X	
HFA Secure	X		4061	X		X	
JSFT	X		8771		X	X	X
JSFT	X		8772		X	X	X
LAS Cloud Service	X		8602	X			
LDAP Server	X		389		X	X	X
Manager E	X		7000	X			
MEB SIP	X		15060		X		X
NAT traversal (NAT-T)		X	4500	X			
NTP		X	123	X			

Beschreibung	TCP	UDP	Portnummer	OpenScape Business X	UC Booster Card	OpenScape Business S	UC Booster Server
Openfire Admin (https)	X		9091		X	X	X
OSBiz Multisite	X		8778		X	X	X
OSBiz myReports (http)	X		8101		X	X	X
OSBiz Status Server	X		8808	X		X	X
OSBiz User Portal	X	X	8779		X	X	X
Postgres	X		5432	X	X	X	X
RTP		X	29100:30530	X	X	X	X
SIP (server)	X	X	5060	X		X	
SIP TLS SIPQ (server)	X		5061	X		X	
SIP TLS Subscriber (server)	X		5062	X		X	
SNMP (Get/Set)		X	161	X		X	
SNMP (Traps)		X	162	X		X	
SSDP	X		3011	X		X	X
TFTP		X	69		O	O	O
VSL	X		8770		X	X	X
Webadmin for Clients	X		8803	X	X	X	X
XMPP Connection Manager	X		5262		X	X	X
XMPP Server	X		5269		X	X	X
Webbased Clients							
Webbased Clients (http)	X		8801	X	X	X	X
Webbased Clients (https)	X		8802	X	X	X	X

INFO: Aus Sicherheitsgründen wird empfohlen für die Webbased Clients ausschließlich https zu verwenden und ein Port Forwarding von extern TCP/443 nach intern TCP/8802 einzurichten.

6 Erstinstallation OpenScape Business UC Booster

Beschrieben wird die erstmalige Installation und Konfiguration von OpenScape Business UC Booster an das OpenScape Business Kommunikationssystem X3/X5/X8. Dabei ist zu unterscheiden, ob für die Nutzung der UC Booster Funktionalität die OpenScape Business UC Booster Card oder der OpenScape Business UC Booster Server verwendet werden soll.

Die Erstinstallation von OpenScape Business UC Booster wird mit dem Administrationsprogramm OpenScape Business Assistant (Web-based Management, kurz WBM genannt) durchgeführt.

Die ausführliche Administration der über die Erstinstallation hinausgehenden Leistungsmerkmale finden Sie in den anschließenden Kapiteln.

Erstinstallation OpenScape Business UC Booster Card

Die OpenScape Business UC Booster Card wird in das OpenScape Business Kommunikationssystems X3/X5/X8 montiert und für den Betrieb konfiguriert. Anschließend wird die Konfiguration der OpenScape Business UC Booster Funktionalität durchgeführt.

Die Erstinstallation unterscheidet sich in ihren Installationsschritten darin, ob die UC Booster Card zusammen mit dem OpenScape Business Kommunikationssystem X3/X5/X8 erstmalig in Betrieb genommen wird oder nachträglich in ein bereits konfiguriertes OpenScape Business Kommunikationssystem X3/X5/X8 integriert wird.

Übersicht über die Installationsschritte für beide Möglichkeiten:

Integration in neues Kommunikationssystem	Integration in bestehendes Kommunikationssystem
	Sicherung der Konfigurationsdaten des Kommunikationssystems
Montage der UC Booster Card Die UC Booster Card wird in das OpenScape Business Kommunikationssystems X3/X5/X8 montiert. Beschreibung siehe OpenScape Business Servicedokumentation, Montage der Hardware - Beschreibung der Baugruppen.	Montage der UC Booster Card Die UC Booster Card wird in das OpenScape Business Kommunikationssystems X3/X5/X8 montiert. Beschreibung siehe OpenScape Business Servicedokumentation, Montage der Hardware - Beschreibung der Baugruppen.

Integration in neues Kommunikationssystem	Integration in bestehendes Kommunikationssystem
Konfiguration der UC Booster Card Die Konfiguration der UC Booster Card wird zusammen mit der Erstinstallation des OpenScape Business Kommunikationssystems X3/X5/X8 durchgeführt. Beschreibung siehe *Integration ins Kunden-LAN*.	Konfiguration der UC Booster Card Die Konfiguration der UC Booster Card wird nachträglich an einem bereits konfigurierten OpenScape Business Kommunikationssystems X3/X5/X8 durchgeführt. Beschreibung siehe *Integration ins Kunden-LAN*. Für die Besonderheiten bei der Konfiguration siehe *Konfiguration der UC Booster Card*
Basiskonfiguration Die Basiskonfiguration wird zusammen mit der Erstinstallation des OpenScape Business Kommunikationssystems X3/X5/X8 durchgeführt. Beschreibung siehe *Basiskonfiguration*.	Basiskonfiguration Die Basiskonfiguration wird nachträglich an einem bereits konfigurierten OpenScape Business Kommunikationssystems X3/X5/X8 durchgeführt. Beschreibung siehe *Basiskonfiguration*. Für die Besonderheiten bei der Basiskonfiguration siehe *Basiskonfiguration*
Abschließende Tätigkeiten Die abschließenden Tätigkeiten (inkl. Lizenzierung der UC Clients) werden zusammen mit der Erstinstallation des OpenScape Business Kommunikationssystems X3/X5/X8 durchgeführt. Beschreibung siehe *Abschließende Tätigkeiten*.	Abschließende Tätigkeiten Die abschließenden Tätigkeiten (inkl. Lizenzierung der UC Clients) werden zusammen mit der Erstinstallation des OpenScape Business Kommunikationssystems X3/X5/X8 durchgeführt. Beschreibung siehe *Abschließende Tätigkeiten*. Für die Besonderheiten bei den abschließenden Tätigkeiten siehe *Abschließende Tätigkeiten*

Erstinstallation OpenScape Business UC Booster Server

Der OpenScape Business UC Booster Server wird zusammen mit dem OpenScape Business Kommunikationssystem X3/X5/X8 in das Kunden-LAN integriert.

Für den OpenScape Business UC Booster Server wird auf dem Linux-Betriebssystem SLES 11 SP3 64 Bit die OpenScape Business Kommunikationssoftware installiert, die die OpenScape Business UC Booster Funktionalität zur Verfügung stellt. Die Kommunikationssoftware kann direkt auf einem Linux-Server oder in einer virtuellen Umgebung mit VMware vSphere betrieben werden. Die Installation des Linux-Betriebssystems ist beschrieben in der Installationsanleitung *OpenScape Business, Installation Linux Server*.

Der OpenScape Business UC Booster Server hat ein eigenes WBM. Dieses WBM wird für Software-Update, Sicherung der Konfigurationsdaten und Diagnose des OpenScape Business UC Booster Servers verwendet. Die Erstinstallation des OpenScape Business UC Booster Servers wird mit dem WBM des Kommunikationssystems durchgeführt.

Die Erstinstallation unterscheidet sich in ihren Installationsschritten darin, ob der UC Booster Server zusammen mit dem OpenScape Business Kommunikationssystem X3/X5/X8 erstmalig in Betrieb genommen wird oder nachträglich an ein bereits konfiguriertes OpenScape Business Kommunikationssystem X3/X5/X8 angeschlossen wird.

Übersicht über die Installationsschritte für beide Möglichkeiten:

Integration in neues Kommunikationssystem	Integration in bestehendes Kommunikationssystem
	Sicherung der Konfigurationsdaten des Kommunikationssystems
Installation des Linux-Servers Die Installation des Linux-Servers ist in der OpenScape Business Linux-Server Installationsanleitung beschrieben.	Installation des Linux-Servers Die Installation des Linux-Servers ist in der OpenScape Business Linux-Server Installationsanleitung beschrieben.
Installation der Kommunikationssoftware	*Installation der Kommunikationssoftware*
Funktionskontrolle mit dem OpenScape Observer	*Funktionskontrolle mit dem OpenScape Observer*
Konfiguration des UC Booster Servers Die Konfiguration des UC Booster Servers wird zusammen mit der Erstinstallation des OpenScape Business Kommunikationssystems X3/X5/X8 durchgeführt. Beschreibung siehe *Integration ins Kunden-LAN*.	Konfiguration des UC Booster Servers Die Konfiguration des UC Booster Servers wird nachträglich an einem bereits konfigurierten OpenScape Business Kommunikationssystems X3/X5/X8 durchgeführt. Beschreibung siehe *Integration ins Kunden-LAN*. Für die Besonderheiten bei der Konfiguration siehe *Konfiguration des UC Booster Servers*
Basiskonfiguration Die Basiskonfiguration wird zusammen mit der Erstinstallation des OpenScape Business Kommunikationssystems X3/X5/X8 durchgeführt. Beschreibung siehe *Basiskonfiguration*.	Basiskonfiguration Die Basiskonfiguration wird nachträglich an einem bereits konfigurierten OpenScape Business Kommunikationssystems X3/X5/X8 durchgeführt. Beschreibung siehe *Basiskonfiguration*. Für die Besonderheiten bei der Basiskonfiguration siehe *Basiskonfiguration*
Abschließende Tätigkeiten Die abschließenden Tätigkeiten (inkl. Lizenzierung der UC Clients) werden zusammen mit der Erstinstallation des OpenScape Business Kommunikationssystems X3/X5/X8 durchgeführt. Beschreibung siehe *Abschließende Tätigkeiten*.	Abschließende Tätigkeiten Die abschließenden Tätigkeiten (inkl. Lizenzierung der UC Clients) werden zusammen mit der Erstinstallation des OpenScape Business Kommunikationssystems X3/X5/X8 durchgeführt. Beschreibung siehe *Abschließende Tätigkeiten*. Für die Besonderheiten bei den abschließenden Tätigkeiten siehe *Abschließende Tätigkeiten*

6.1 Voraussetzungen für die Erstinstallation

Die Erfüllung der Voraussetzungen für die Erstinstallation gewährleistet den Betrieb von OpenScape Business UC Booster.

Allgemein

Abhängig von der verwendeten Hardware (Telefone,...) und der vorhandenen Infrastruktur gelten folgende allgemeine Voraussetzungen:

- Das OpenScape Business Kommunikationssystem X3/X5/X8 ist konfiguriert und betriebsbereit.
- Die LAN-Infrastruktur (Internet-Router, Switche, usw.) ist vorhanden und nutzbar.
- Die IP-Telefone sind an das Kunden-LAN angeschlossen.
- Ein Breitband-Internet-Zugang ist empfohlen für Software-Update und Remote-Zugang.
- Alle für OpenScape Business UC Booster benötigten Lizenzen sind vorhanden (z. B. UC Clients, Gate View, Directory Services, usw...). Bei einer Integration in ein bereits lizenziertes Kommunikationssystem gibt es keine Activation Period mehr.
- Ein IP-Adressen-Schema ist vorhanden und bekannt.
- Ein Rufnummernplan ist vorhanden und bekannt.

Für UC Booster Card

Folgende Voraussetzungen sind für den Betrieb der UC Booster Card zu beachten.

- OpenScape Business Hardware:
  Die UC Booster Card ist installiert.
- Switch:
  Der Switch, über den die UC Booster Card mit dem Kommunikationssystem verbunden ist, sollte IPv6-fähig sein, damit die UC Booster Card während der Erstinstallation eine IP-Adresse erhält.
  Ist der Switch nicht IPv6-fähig, blinkt die rote LED des Kommunikationssystems. In diesem Fall muss der Admin-Port des Systems über ein zusätzliches Ethernet-Kabel mit dem zweiten LAN-Port der UC Booster Card verbunden werden. Dadurch erhält die UC Booster Card automatisch eine IPv4-IP-Adresse über das IPv6-Protokoll. Sobald die UC Booster Card über IP erreichbar ist, erlischt die rote LED des Konnumikationssystems. Anschließend kann die gewünschte IP-Adresse für die UC Booster Card während der Erstinstallation eingegeben werden. Die Kommunikation zwischen System und UC Booster Card findet jetzt über die IPv4-Verbindung des Switchs statt.

  INFO: Das zusätzliche Ethernet-Kabel sollte für den Fall eines Neustarts oder eines Reloads gesteckt bleiben.

- Lüfterkit:
  Die UC Booster Card benötigt einen zusätzlichen Lüfter. Das Lüfterkit ist abhängig vom Kommunikationssystem.
- Gehäusekappe:
  Bei OpenScape Business X3W wird für das UC Booster Card Lüfterkit eine neue Gehäusekappe benötigt.
  Bei der Migration von HiPath 3000 Systemen werden für OpenScape Business X3W/X5W und X3R/X5R neue Gehäusekappen für das UC Booster Card Lüfterkit benötigt.

- Kommunikationssoftware:
  Die Software des Kommunikationssystems muss auf die neuerste, freigegebene Software-Version aktualisiert werden. Dabei ist zu beachten, dass das Image inkl. der UC Booster Card Software verwendet wird.
- Webbrowser:
  Für die Erstinstallation der UC Booster Card mit dem OpenScape Business Assistant (WBM) wird der Admin-PC verwendet. Das WBM ist browserbasiert und somit betriebssystemunabhängig. Es wird eine Bildschirmauflösung von 1024x768 oder höher benötigt.
  Es werden nachfolgende HTML 5 fähige Web-Browser unterstützt:
  – Microsoft Internet Explorer ab Version 10
  – Mozilla Firefox ab Version 17
  Falls eine ältere Webbrowser-Version installiert ist, muss eine aktuelle Version installiert werden, bevor mit der Erstinstallation begonnen werden kann.

Für UC Booster Server

Folgende Voraussetzungen sind für den Betrieb des UC Booster Servers zu beachten.

- Linux-Server:
  Der für OpenScape Business S benötigte Linux-Server wurde nach der OpenScape Business V1 Linux Server Installationsanleitung installiert, ist betriebsbereit und in das Kunden-LAN integriert..
- OpenScape Business Kommunikationssoftware:
  Die Installations-DVD mit der OpenScape Business Kommunikationssoftware ist vorhanden. Nach der Software-Installation muss die Software des Kommunikationssystems und die Kommunikationssoftware des UC Booster Servers separat auf den gleichen, neuersten, freigegebenen Software-Version aktualisiert werden.
- DVD mit Linux-Betriebssystem SLES 11 SP3 64 Bit
  Die Linux-DVD wird ggf. bei der Installation der OpenScape Business Kommunikationssoftware benötigt, wenn Software-Pakete (RPM) nachinstalliert werden müssen, die für die Kommunikationssoftware benötigt werden.
- Webbrowser:
  Für die Erstinstallation des UC Booster Servers mit dem OpenScape Business Assistant (WBM) kann der Linux-Server oder der Admin-PC verwendet werden. Das WBM ist browserbasiert und somit betriebssystemunabhängig. Es wird eine Bildschirmauflösung von 1024x768 oder höher benötigt.
  Es werden nachfolgende HTML 5 fähige Web-Browser unterstützt:
  – Microsoft Internet Explorer ab Version 10 (Admin-PC)
  – Mozilla Firefox ab Version 17 (Linux-Server / Admin-PC)
  Falls eine ältere Webbrowser-Version installiert ist, muss eine aktuelle Version installiert werden, bevor mit der Erstinstallation begonnen werden kann.
- Firewall:
  Beim Anschluss an das Internet ist für den Linux-Server eine Firewall nötig, um unautorisierten Zugriff von außen zu verhindern. Nach der Installation von

Linux ist die Linux-Firewall aktiviert. Durch das Installationsprogramm der Kommunikationssoftware wird die Firewall so angepasst, dass sie den Betrieb der Kommunikationssoftware zulässt. Die Ports für die Kommunikationssoftware sind geöffnet, alle anderen Ports geschlossen.
Wird im Netzwerk eine externe Firewall eingesetzt, müssen die Linux-Firewall deaktiviert und die für die Kommunikationssoftware erforderlichen Adressen und Ports freigegeben werden (siehe *Verwendete Ports*).

6.2 Sicherung der Konfigurationsdaten des Kommunikationssystems

Bevor OpenScape Business UC Booster installiert wird, sollte unbedingt eine Sicherung der bestehenden Konfigurationsdaten des OpenScape Business Kommunikationssystems durchgeführt werden.

Die Sicherung erfolgt am WBM des OpenScape Business Kommunikationssystems.

Es kann auf unterschiedliche Backup-Medien gesichert werden (wie z. B. auf ein USB-Medium oder ein Netzlaufwerk).

6.2.1 Wie Sie die Datensicherung durchführen

Voraussetzungen

- Sie sind am WBM des Kommunikationssystems mit dem Profil **Advanced** angemeldet.
- Für eine Datensicherung auf einem USB-Medium muss das USB-Medium an der USB-Server-Schnittstelle des Kommunikationssystems angeschlossen sein.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Datensicherung**.

2) Klicken Sie im Navigationsbaum auf **Backup - sofort**.

3) Geben Sie im Bereich **Name** im Feld **Kommentar** einen Kommentar für das Backup-Set ein, um das Backup-Set bei einer möglichen Wiederherstellung leichter identifizieren zu können. Vermeiden Sie bei der Eingabe Umlaute und Sonderzeichen.

4) Aktivieren Sie im Bereich **Geräte** das Ziellaufwerk, auf dem das Backup-Set gespeichert werden soll.

5) Klicken Sie auf **OK & Weiter**. In einem weiteren Fenster wird Ihnen der Fortschritt der Sicherung angezeigt.

6) Die Sicherung ist erfolgreich, wenn die Meldung **Sicherung erfolgreich ausgeführt!** erscheint. Klicken Sie auf **Beenden**.

7) Wenn Sie als Backup-Medium einen USB-Stick verwenden, warten Sie ab, bis die LED des USB-Sticks aufhört zu blinken. Erst dann ist die Sicherung

erfolgreich auf dem USB-Stick gespeichert. Entfernen Sie anschließend den USB-Stick.

8) Die Datensicherung mit dem WBM ist nun abgeschlossen. Beenden Sie das WBM, indem Sie rechts oben auf den Link **Abmelden** klicken und anschließend das Fenster schließen.

6.3 Inbetriebnahme UC Booster Card

Die Inbetriebnahme der UC Booster Card umfasst die Montage in das OpenScape Business Kommunikationssystem und die erstmalige Konfiguration für den korrekten Betrieb.

Nach erfolgreicher Konfiguration muss ein Software-Update durchgeführt werden.

6.3.1 Montage der UC Booster Card

Die UC Booster Card wird in das OpenScape Business Kommunikationssystem integriert. Der Steckplatz der UC Booster Card ist abhängig vom Kommunikationssystem.

Die Montage der UC Booster Card ist in der Servicedokumentation, Montage der Hardware im Kapitel "Beschreibung der Baugruppen" ausführlich beschrieben.

Die UC Booster Card kann in folgende OpenScape Business Kommunikationssysteme integriert werden:

- OpenScape Business X3R und X5R (OCCMR)
  UC Booster Card mit zusätzlichem Lüfterkit.
- OpenScape Business X3W und X5W (OCCM)
  UC Booster Card mit zusätzlichem Lüfterkit.
  Für OpenScape Business X3W wird für den Lüfterkit zusätzlich eine neue Gehäusekappe benötigt.
- OpenScape Business X8 (OCCL)
  UC Booster Card mit zusätzlichem Lüfterkit.

6.3.2 Konfiguration der UC Booster Card

Während der Konfiguration werden die grundlegenden Einstellungen für den Betrieb der UC Booster Card festgelegt.

Die Konfiguration der UC Booster Card wird mit dem Wizard **Erstinstallation** des WBM des Kommunikationssystems durchgeführt. Die Beschreibung der Konfiguration finden Sie im Kapitel Erstinstallation OpenScape Business X3/X5/X8.

Der Wizard **Erstinstallation** des WBM umfasst die erstmalige Konfiguration des gesamten Kommunikationssystems. Für den Betrieb der OpenScape Business UC Booster Card sind folgende Konfigurationsanteile wichtig:

- IP-Adresse der UC Booster Card
  Die UC Booster Card benötigt eine eigenständige IP-Adresse aus dem Netzsegment des Kommunikationssystems.
- Auswahl der UC-Lösung
  Es kann ausgewählt werden, ob die mit der UC Booster Card zur Verfügung gestellte UC-Lösung UC Suite genutzt werden soll.

Das Ändern der IP-Adresse der UC Booster Card oder der UC-Lösung führt zu einem Neustart des Kommunikationssystems.

6.3.3 Software-Update für die UC Booster Card

Für den korrekten Betrieb der UC Booster Card muss die Software des Kommunikationssystems aktualisiert werden. Dadurch werden alle fehlenden Software-Komponenten für die UC Booster Card nachinstalliert.

Ist die Software des Kommunikationssystems bereits auf dem aktuellen Stand, muss das System nochmals mit der aktuellen Software aktualisiert werden, damit alle für die UC Booster Funktionalität benötigten Komponenten nachinstalliert werden.

Das Software-Update kann einerseits über das Internet durchgeführt werden oder andererseits über eine Image-Datei, die vom Software Download Server bezogen werden kann. Beim Update über die Image-Datei ist darauf zu achten, dass diejenige Image-Datei verwendet wird, die die UC Booster Card Anteile enthält (osbiz_v1_ocab.tar).

6.3.3.1 Wie Sie ein Software-Update durchführen

Voraussetzungen

- Ein Zugang zum Internet ist vorhanden.
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Software Update > Update via Internet**. Es wird Ihnen die aktuell installierte Softwareversion angezeigt.

3) Klicken Sie auf **OK & Weiter**.

4) Lesen Sie sich die Lizenzvereinbarung (EULA) durch und aktivieren Sie anschließend das Optionsfeld **Ich stimme der Lizenzvereinbarung zu**.

5) Klicken Sie auf **OK & Weiter**.

6) Aktivieren Sie das Optionsfeld **Start der Aktion - Sofort / Sofort nach der Übertragung**.

7) Klicken Sie auf **OK & Weiter**. Das Software-Update wird im Hintergrund in das Kommunikationssystem geladen und nach der Übertragung automatisch aktiviert. Nach zwei Neustarts ist die Software aktualisiert.

INFO: Sie können das Browser-Fenster jederzeit schließen.

8) Den aktuellen Status des Updates können Sie mit dem WBM unter **Service-Center > Software-Update > Status** abfragen.

6.4 Inbetriebnahme UC Booster Server

Die Inbetriebnahme des UC Booster Servers umfasst die Installation der OpenScape Business Kommunikationssoftware auf dem Linux-Server und die erstmalige Konfiguration für den korrekten Betrieb.

Nach erfolgreicher Konfiguration muss ein Software-Update durchgeführt werden.

6.4.1 Installation der Kommunikationssoftware

Die OpenScape Business Kommunikationssoftware wird auf dem Linux-Server mit Hilfe der OpenScape Business DVD installiert.

Achten Sie darauf, dass die zu konfigurierenden IP-Adressen und Netzmasken zu dem Kunden-LAN passen.

DHCP-Server

Ein DHCP-Server weist den IP-Teilnehmern (IP-Telefone, PCs, usw.) automatisch eine IP-Adresse zu und versorgt sie mit netzwerkspezifischen Daten, wie z.B. der IP-Adresse des Standard-Gateways.

Als DHCP-Server kann ein externer DHCP-Server genutzt werden (z.B. der DHCP-Server des Internet-Routers oder des Kommunikationssystems) oder der DHCP-Server des Linux-Servers. Soll der DHCP-Server des Linux-Servers verwendet werden, muss der externer DHCP-Server deaktiviert werden. Die Konfiguration des Linux-DHCP-Servers kann während der Installation der OpenScape Business Kommunikationssoftware durchgeführt werden.

Virtuelle Umgebung

Die Kommunikationssoftware kann in einer virtuellen Umgebung laufen. Dazu wird auf dem Server-PC zuerst die Virtualisierungssoftware (Hostbetriebssystem) installiert und konfiguriert. Anschließend wird Linux als Gastbetriebssystem installiert. Innerhalb des Linux-Betriebssystems wird zuletzt die Kommunikationssoftware installiert (siehe hierzu *OpenScape Business V1, Linux Server, Installationsanleitung*).

Einsatz von Snapshots auf Virtuellen Maschinen (VM):

Snapshots können ein wertvoller Wartungsmechanismus sein, z. B. um einen schnellen Rollback auf einen vordefinierten Betriebszustand der VM durchzuführen, nachdem ein Massenverteiler-Skript fehlgeschlagen ist.

- Snapshots dürfen nicht während des laufenden Betriebes durchgeführt werden. Während ein Snapshot gezogen wird, wird der aktuelle Betriebszustand der virtuellen Maschine eingefroren. Daher können verbundene Endgeräte und Applikationen, wie IP-Telefone oder die UC-Clients die Verbindung zum Server verlieren.
- Snapshots können zur Folge haben, dass interne Serverprozesse ihre Synchronisation verlieren und ein stabiler Betrieb des Kommunikationssystems nicht mehr gewährleistet ist. Daher sollte im Anschluss an den Snapshot ein Server-Neustart mit in das Wartungsfenster eingeplant werden.
- Vorherige Snapshots dürfen auf der Produktionsumgebung während des normalen Betriebes nicht verbleiben.
- Snapshots können während eines vorgesehenen Wartungsfensters oder im Rahmen der Installation gezogen werden.
- Snapshots werden intern von Backup-Tools wie VDP oder VDR genutzt. Es muss sichergestellt sein, dass diese Backup-Vorgänge außerhalb der Geschäftszeiten geplant werden und dass Snapshots, die durch diese Tools generiert werden, am Ende des Vorgangs gelöscht werden.

Weitere Informationen bezüglich Snapshots können der VMware Knowledge Base (KB) entnommen werden. Ein guter Einstiegspunkt ist der KB-Artikel 1025279 - Best Practices for virtual machine snapshots in the VMware environment (`http://kb.vmware.com/kb/1025279`).

6.4.1.1 Wie Sie die Kommunikationssoftware installieren

Voraussetzungen

- Das Betriebssystem SLES 11 SP3 64 Bit wurde korrekt auf dem Linux-Server installiert und gestartet.
- DVD mit OpenScape Business Kommunikationssoftware.
- DVD mit Linux-Betriebssystem SLES 11 SP3 64 Bit für die eventuell benötigte Nachinstallation von Software-Pakete (RPM).
- Die Root-Zugangsdaten (Benutzername und Passwort) für die Anmledung am Linux-Server liegen vor.

> ***WICHTIG:*** Die OpenScape Business Kommunikationssoftware überschreibt bei der Installation evtl. vorhandene Konfigurationsdateien (z. B. für DHCP, FTP, Postfix, usw.).

Schritt für Schritt

1) Melden Sie sich am Linux-Server mit Root-Rechten an.

2) Legen Sie die OpenScape Business DVD in das DVD-Laufwerk ein.

3) Bestätigen Sie den Hinweis mit **Run**. Es erscheint das Fenster "Welcome".

4) Wählen Sie die gewünschte Setup-Sprache aus (z. B. **english**) und klicken Sie auf **Start**. Die weitere Installation ist für die englische Sprachauswahl beschrieben.

5) Wählen Sie aus der Liste das gewünschte Produkt aus und klicken Sie auf **Select**. Es wird geprüft, ob die Hardware alle Voraussetzungen für die Installation erfüllt. Bei geringfügiger Unterschreitung der Voraussetzungen erfolgt eine Warnung. Nach Bestätigung kann die Installation fortgesetzt werden. Bei schwerwiegender Unterschreitung wird die Installation automatisch abgebrochen.

6) Es wird untersucht, ob zusätzliche RPM-Pakete installiert werden müssen. Falls ja, bestätigen Sie dies mit **Confirm**. Später muss in diesem Fall auf die SLES 11 DVD gewechselt werden.

7) Es erscheint ein Fenster mit den Lizenzbestimmungen (EULA, End User License Agreement). Lesen Sie sich die Lizenzbestimmungen durch und akzeptieren Sie die Lizenzbestimmungen mit **Yes**.

8) Wenn im Kunden-LAN bereits ein DHCP-Server vorhanden ist (z.B. der DHCP-Server des Internet-Routers), brechen Sie hier die Konfiguration des Linux-DHCP-Servers mit **No** ab. Fahren Sie mit Schritt 12 fort.

INFO: Damit auch bei Nutzung eines externen DHCP-Servers die Software der Systemtelefone automatisch aktualisiert werden kann, haben Sie zwei Möglichkeiten:

a) bei jedem Systemtelefon muss als DLS-Adresse die IP-Adresse des Linux-Servers eingetragen werden.

b) bei dem externen DHCP-Server müssen die netzwerkspezifischen Daten eingetragen werden. Die Parameter dazu finden Sie unter `/var/log/OPTI.txt`.

---

9) Wenn Sie den Linux-DHCP-Server nutzen wollen, Klicken Sie auf **Yes**, um den Linux-DHCP-Server zu aktivieren und zu konfigurieren.

10) Geben Sie folgende Werte ein (vorbelegt mit Standard-Werten):

- **Default Route**: IP-Adresse des Standard-Gateways, in der Regel die IP-Adresse des Internet-Routers, z.B. `192.168.5.1`.
- **Domain** (optional): die während der Linux-Installation angegebene Domäne, z.B. `<customer>.com`
- **DNS-Server** (optional): die während der Linux-Installation angegebene IP-Adresse des DNS-Servers. Ist im internen Netz kein DNS-Server vorhanden, können Sie hier die IP-Adresse des Internet-Routers eintragen (z. B. `192.168.5.1`).
- **SNTP Server**: IP-Adresse des internen oder externen NTP-Servers.
- **DLS/DLI Server**: IP-Adresse des DLS-Servers, d.h. die IP-Adresse des Linux-Servers (z.B. `192.168.5.10`).

- **Subnet**: das zum IP-Adressbereich passende Subnetz, z.B. `192.168.5.0`.
- **Netmask**: die während der Linux-Installation angegebene Subnetzmaske des Linux-Servers, z.B. `255.255.255.0`.
- **IP range begin** und **IP range end**: IP-Adressbereich, aus dem der DHCP-Server die IP-Adressen vergeben darf, z.B. `192.168.5.100` bis `192.168.5.254`.

11) Klicken Sie auf **Continue**.

12) Nach der Installation ist ein Neustart des Linux-Betriebssystems notwendig. Aktivieren Sie das Kontrollkästchen **PC Reboot** und bestätigen Sie mit **Continue**.

13) Wenn zusätzliche RPM-Pakete installiert werden müssen, werden Sie aufgefordert, die SLES 11 DVD einzulegen. Legen Sie die DVD ein und bestätigen Sie mit **Continue**. Legen Sie nach erfolgreicher Installation der RPM-Pakete wieder die OpenScape Business DVD ein und bestätigen Sie mit **Continue** und anschließend mit **Run**.

14) Die OpenScape Business Kommunikationssoftware wird installiert. Anschließend führt das Betriebssystem automatisch einen Neustart durch.

15) Melden Sie sich nach dem Neustart mit dem Benutzerkonto an, das zuvor bei der Linux-Installation eingerichtet wurde.

16) Klicken Sie auf dem Desktop mit der rechten Maustaste auf das Symbol des DVD-Laufwerks und wählen Sie den Menüpunkt **Eject**. Entfernen Sie die OpenScape Business DVD aus dem DVD-Laufwerk.

INFO: Es dauert einige Minuten, bis alle Komponenten der OpenScape Business Kommunikationssoftware aktiv sind. Mit dem OpenScape Observer können Sie kontrollieren, wann die OpenScape Business Kommunikationssoftware betriebsbereit ist.

6.4.2 Funktionskontrolle mit dem OpenScape Observer

Mit dem Programm OpenScape Observer können Sie kontrollieren, ob OpenScape Business betriebsbereit ist.

Der OpenScape Observer kann vom Admin-PC oder von einem Client-PC im internen Netz gestartet werden. Dazu muss das Programm aus dem Service-Center des WBM auf den PC kopiert werden.

6.4.2.1 Wie Sie den OpenScape Observer auf den PC kopieren

Voraussetzungen

- Die OpenScape Business Kommunikationssoftware ist installiert.
- Die aktuellste Java Runtime Environment Version ist auf dem PC installiert.

Schritt für Schritt

1) Starten Sie auf dem PC den Webbrowser und rufen Sie die Anmeldeseite des WBM unter folgender Adresse auf:

`https://<IP-Adresse des Linux-Servers>`, z. B. `https://192.168.5.10`.

2) Wenn der Webbrowser ein Problem mit einem Sicherheitszertifikat meldet, installieren Sie das Zertifikat (am Beispiel der Internet Explorers V10).

a) Schließen Sie den Webbrowser.

b) Öffnen Sie den Webbrowser mit Administratorrechten, indem Sie mit der rechten Maustaste auf das Webbrowser-Symbol klicken und im Kontextmenü den Eintrag **Als Administrator ausführen** auswählen.

c) Erlauben Sie die Benutzerkontensteuerung.

d) Rufen Sie die Anmeldeseite des WBM unter folgender Adresse auf:

`https://<IP-Adresse des Linux-Servers>`, z. B. `https://192.168.5.10`.

e) Klicken Sie auf **Laden dieser Website fortsetzen**.

f) Klicken Sie auf die Meldung **Zertifikatsfehler** in der Navigationsleiste des Webbrowsers.

g) Klicken Sie auf **Zertifikate anzeigen**.

h) Klicken Sie auf **Zertifikat installieren** (nur sichtbar mit Administratorrechten).

i) Wählen Sie die Option **Lokaler Computer** und bestätigen Sie mit **Weiter**.

j) Wählen Sie die Option **Alle Zertifikate in folgendem Speicher speichern**, klicken Sie auf **Durchsuchen** und geben Sie **Vertrauenswürdige Stammzertifizierungsstellen** an.

k) Bestätigen Sie mit **OK** und anschließend mit **Weiter** und **Fertigstellen**.

l) Bestätigen Sie den Zertifikatimport mit **OK** und schließen Sie das Zertifikatsfenster mit **OK**.

m) Schließen Sie den Webbrowser.

n) Starten Sie den Webbrowser erneut (ohne Administratorrechte) und rufen Sie die Anmeldeseite des WBM unter folgender Adresse auf:

`https://<IP-Adresse des Linux-Servers>`, z. B. `https://192.168.5.10`.

3) Klicken Sie oben rechts auf das Sprachkürzel und wählen Sie aus dem Menü die Sprache aus, in der die Oberfläche des WBM angezeigt werden soll. Die Anmeldeseite wird in der ausgewählten Sprache angezeigt.

4) Geben Sie im ersten Feld unter **Login** den Standard-Benutzernamen `administrator@system` für den Zugang als Administrator ein.

> ***INFO:*** Wenn Sie nach der Eingabe von `administrator` die Tabulator-Taste drücken, wird `@system` automatisch ergänzt.

5) Geben Sie im zweiten Feld unter **Login** das Standard-Passwort `administrator` für den Zugang als Administrator ein.

6) Klicken Sie auf **Login**.

7) Sie werden aufgefordert, das Standard-Passwort zu ändern.

a) Geben Sie im Feld **Passwort** nochmal das Standard-Passwort `administrator` ein.

b) Geben Sie in den Feldern **Neues Passwort** und **Neues Passwort bestätigen** ein neues Passwort ein, um das System gegen Missbrauch zu schützen. Berücksichtigen Sie Groß-/Kleinschreibung und den Zustand der Taste **Num**. Das Passwort erscheint verdeckt durch Sternchen (*).

> ***INFO:*** Das Passwort muss mindestens 8 Zeichen lang sein und eine Ziffer enthalten. Bitte merken Sie sich Ihr neues Passwort genau.

8) Klicken Sie auf **Login**.

9) Klicken Sie in der Navigationsleiste auf **Service-Center**.

10) Klicken Sie im Bereich **Software** auf den Eintrag **OpenScape Observer**.

11) Speichern Sie die Datei `OsoObserver.jar` auf dem PC in einem Verzeichnis Ihrer Wahl.

6.4.2.2 Wie Sie den OpenScape Observer vom PC starten

Voraussetzungen

- Die Datei `OsoObserver.jar` ist auf dem Client-PC abgelegt.

Schritt für Schritt

1) Navigieren Sie auf dem PC zum Ablagepfad des OpenScape Observers.

2) Doppelklicken Sie auf die Datei `OsoObserver.jar`. Der OpenScape Observer öffnet sich als kleines Fenster in der linken oberen Ecke des Bildschirms.

3) Geben Sie im Feld des OpenScape Observers die IP-Adresse des Linux-Servers ein, auf dem die OpenScape Business Kommunikationssoftware installiert ist (z. B. `192.168.5.10`).

4) Klicken Sie auf **Connect OSO**.

5) Es öffnet sich ein weiteres Fenster mit folgendem Inhalt:

- IP-Adresse des Linux-Servers (in der Kopfzeile)
- Versionsnummer der installierten OpenScape Business Kommunikationssoftware
- Version des Linux-Server-Betriebssystems
- Auslastung der home-Partition (`HD`) und des Arbeitsspeichers (`RAM`) des Linux-Servers in Prozent
- Abkürzung des installierten Produkts (z. B. `S` für OpenScape Business S und `B` für UC Booster Server)

6) In dem Fenster werden Sie zusätzlich mit einer LED-Anzeige über den Status von OpenScape Business informiert:

- Rote LED: Die OpenScape Business Systemkomponenten können nicht gestartet werden - OpenScape Business ist nicht betriebsbereit
- Gelbe LED: Die OpenScape Business Systemkomponenten werden gestartet - OpenScape Business ist noch nicht betriebsbereit
- Grüne LED: Die OpenScape Business Systemkomponenten sind gestartet - OpenScape Business ist betriebsbereit

6.4.3 Konfiguration des UC Booster Servers

Während der Konfiguration werden die grundlegenden Einstellungen für den Betrieb des UC Booster Servers festgelegt.

Die Konfiguration des UC Booster Servers wird mit dem Wizard **Erstinstallation** des WBM des Kommunikationssystems durchgeführt. Die Beschreibung der Konfiguration finden Sie im Kapitel Erstinstallation OpenScape Business X.

Der Wizard **Erstinstallation** des WBM umfasst die erstmalige Konfiguration des gesamten Kommunikationssystems. Für den Betrieb des OpenScape Business UC Booster Servers sind folgende Konfigurationsanteile wichtig:

- Auswahl der UC-Lösung
  Es kann ausgewählt werden, ob die mit dem UC Booster Server zur Verfügung gestellte UC-Lösung UC Suite genutzt werden soll. Dazu muss auch die IP-Adresse des Linux-Servers eingetragen werden.
  Das Ändern der UC-Lösung führt zu einem Neustart des Kommunikationssystems.

Zusätzlich muss am WBM des UC Booster Servers die IP-Adresse des Kommunikationssystems bekannt gegeben werden.

6.4.3.1 IP-Adresse des Kommunikationssystems bekannt geben

Voraussetzungen

- Der UC Booster Server ist in das Kunden-LAN integriert und betriebsbereit.
- Das OpenScape Business Kommunikationssystem ist betriebsbereit.

Schritt für Schritt

1) Starten Sie auf dem Linux-PC den Webbrowser und rufen Sie das WBM des OpenScape Business Servers unter folgender Adresse auf:

`https://<IP-Adresse des Linux-Servers>`, z. B. `https://192.168.1.10`

2) Wenn der Webbrowser ein Problem mit einem Sicherheitszertifikat meldet, installieren Sie das Zertifikat (am Beispiel der Internet Explorers V10).

a) Schließen Sie den Webbrowser.

b) Öffnen Sie den Webbrowser mit Administratorrechten, indem Sie mit der rechten Maustaste auf das Webbrowser-Symbol klicken und im Kontextmenü den Eintrag **Als Administrator ausführen** auswählen.

c) Erlauben Sie die Benutzerkontensteuerung.

d) Rufen Sie das WBM des OpenScape Business Servers unter folgender Adresse auf:

`https://<IP-Adresse des Linux-Servers>`, z. B. `https://192.168.1.10`

e) Klicken Sie auf **Laden dieser Website fortsetzen**.

f) Klicken Sie auf die Meldung **Zertifikatsfehler** in der Navigationsleiste des Webbrowsers.

g) Klicken Sie auf **Zertifikate anzeigen**.

h) Klicken Sie auf **Zertifikat installieren** (nur sichtbar mit Administratorrechten).

i) Wählen Sie die Option **Lokaler Computer** und bestätigen Sie mit **Weiter**.

j) Wählen Sie die Option **Alle Zertifikate in folgendem Speicher speichern**, klicken Sie auf **Durchsuchen** und geben Sie **Vertrauenswürdige Stammzertifizierungsstellen** an.

k) Bestätigen Sie mit **OK** und anschließend mit **Weiter** und **Fertigstellen**.

l) Bestätigen Sie den Zertifikatimport mit **OK** und schließen Sie das Zertifikatsfenster mit **OK**.

m) Schließen Sie den Webbrowser.

n) Starten Sie den Webbrowser erneut (ohne Administratorrechte) und rufen Sie das WBM des OpenScape Business Servers unter folgender Adresse auf:

`https://<IP-Adresse des Linux-Servers>`, z. B. `https://192.168.1.10`

3) Klicken Sie oben rechts auf das Sprachkürzel und wählen Sie aus dem Menü die Sprache aus, in der die Oberfläche des WBM angezeigt werden soll. Die Anmeldeseite wird in der ausgewählten Sprache angezeigt.

4) Geben Sie im ersten Feld unter **Login** den Standard-Benutzernamen `administrator@system` für den Zugang als Administrator ein.

INFO: Wenn Sie nach Eingabe von `administrator` in das Feld **Passwort** wechseln, wird `@system` automatisch ergänzt.

---

5) Geben Sie im zweiten Feld unter **Login** das Standard-Passwort `administrator` für den Zugang als Administrator ein.

6) Klicken Sie auf **Login**.

7) Folgende Schritte sind nur einmalig beim ersten Anmelden am WBM nötig:

a) Geben Sie im Feld **Passwort** nochmal das Standard-Passwort `administrator` ein.

b) Geben Sie in den Feldern **Neues Passwort** und **Neues Passwort bestätigen** ein neues Passwort ein, um das System gegen Missbrauch zu schützen. Berücksichtigen Sie Groß-/Kleinschreibung und den Zustand der Tasten `Num` und `CapsLock` (Feststelltaste). Das Passwort erscheint verdeckt durch Sternchen (*).

INFO: Das Passwort muss mindestens 8 Zeichen lang sein und eine Ziffer enthalten. Bitte merken Sie sich Ihr neues Passwort genau.

---

c) Klicken Sie auf **Login**.

d) Wählen Sie das aktuelle Datum aus und tragen Sie die Uhrzeit korrekt ein.

e) Klicken Sie auf **OK & Weiter**. Sie werden automatisch vom WBM abgemeldet.

f) Geben Sie im ersten Feld unter **Login** den Standard-Benutzernamen `administrator@system` für den Zugang als Administrator ein.

INFO: Wenn Sie nach Eingabe von `administrator` in das Feld **Passwort** wechseln, wird `@system` automatisch ergänzt.

---

g) Geben Sie im zweiten Feld unter **Login** Ihr neu definiertes Passwort für den Zugang als Administrator ein.

h) Klicken Sie auf **Login**. Es erscheint die Startseite des WBM.

i) Klicken Sie in der Navigationsleiste auf **Administratoren**.

j) Aktivieren Sie in der **Administratoren-Liste** das Kontrollkästchen vor dem Listeneintrag **Administrator**.

k) Klicken Sie auf **Bearbeiten**.

l) Wählen Sie in der Aufklappliste **Benutzerrolle** das Benutzerprofil **Expert** aus.

m) Klicken Sie auf **OK & Weiter**.

n) Melden Sie sich am WBM ab über den Link **Abmelden** rechts oben.

o) Melden Sie sich erneut am WBM an mit dem Standard-Benutzernamen `administrator@system` und dem neu definierten Passwort.

8) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

9) Klicken Sie im Navigationsbaum auf **Wartung > Konfiguration**.

10) Geben Sie im Register **Gateway IP-Adresse ändern** unter **Gateway IP-Adresse** die IP-Adresse des Kommunikationssystems ein, z. B. `192.168.1.2`.

11) Klicken Sie auf **Übernehmen**.

6.4.4 Software-Update für den UC Booster Server

Für den korrekten Betrieb des UC Booster Servers muss die Software des Kommunikationssystems und die Software der Kommunikationssoftware des UC Booster Servers auf den gleichen Software-Stand aktualisiert werden.

Ist die Software des Kommunikationssystems bereits auf dem aktuellen Stand, muss nur noch die Software des UC Booster Servers aktualisiert werden.

Das Software-Update kann einerseits über das Internet durchgeführt werden oder andererseits über eine Image-Datei, die vom Software Download Server bezogen werden kann. Beim Update des UC Booster Servers über die Image-Datei ist darauf zu achten, dass diejenige Image-Datei verwendet wird, die die UC Booster Server Anteile enthält (osbiz_v1_pcx.tar).

6.5 Basiskonfiguration

Während der Basiskonfiguration werden die wichtigsten Einstellungen für den Betrieb von OpenScape Business UC Booster festgelegt.

Die Basiskonfiguration wird sowohl für die UC Booster Card als auch für den UC Booster Server mit dem Wizard **Basisinstallation** des WBM des Kommunikationssystems durchgeführt. Die Beschreibung der Basiskonfiguration finden Sie im Kapitel Erstinstallation OpenScape Business X.

Die Basiskonfiguration umfasst die Konfiguration des gesamten Kommunikationssystems. Für den Betrieb von OpenScape Business UC Booster sind folgende Konfigurationsanteile wichtig:

- Teilnehmerdaten
  Spezielle Rufnummern, die für den Betrieb von OpenScape Business UC Booster benötigt werden, können angepasst werden. Hier muss z. B. die Rufnummer der UC Suite Sprachbox (VoiceMail) angegeben werden.
- Konfiguration der UC Booster Card
  Ist eine UC Booster Card in das Kommunikationssystem integriert, muss die automatische Konfiguration der UC Booster Card eingeleitet werden.
- Meet-Me-Konferenzeinstellungen
  Mit OpenScape Business UC Booster steht das Leistungsmerkmal Meet-Me-Konferenz zur Verfügung. Die vorbelegte Rufnummer und die vorbelegte Einwahlnummer für die Meet-Me-Konferenz können geändert werden.

6.6 Abschließende Tätigkeiten

Nachdem die Erstinstallation und die Basisinstallation mit dem WBM abgeschlossen sind, müssen noch einige wichtige Einstellungen für den Betrieb von OpenScape Business UC Booster getroffen werden.

Die abschließenden Tätigkeiten werden sowohl für die UC Booster Card als auch für den UC Booster Server mit dem WBM des Kommunikationssystems durchgeführt. Die Beschreibung der abschließenden Tätigkeiten finden Sie in der Online-Hilfe oder in der OpenScape Business Administratordokumentation, Kapitel Erstinstallation OpenScape Business X.

Für den Betrieb von OpenScape Business UC Booster sind folgende abschließende Tätigkeiten wichtig:

- Lizenzen aktivieren und zuordnen
  Um die OpenScape Business UC Booster Funktionalität nutzen zu können, müssen bei einer Integration in ein bereits lizenziertes Kommunikationssystem die Lizenzen sofort aktiviert werden. Bei einer Integration in ein noch nicht lizenziertes Kommunikationssystem sind die Lizenzen innerhalb einer Zeitspanne von 30 Tagen zu aktivieren. Nach erfolgreicher Aktivierung müssen die Lizenzen den Teilnehmern zugeordnet werden. Systemweite Leistungsmerkmale sind in einem Standalone-System bereits mit der Aktivierung freigeschaltet.
- UC Clients zur Installation bereitstellen
  Die UC Clients sind Bestandteil der UC Suite. Die Installationsdateien für die UC Clients sind über das WBM zugänglich und können den IP-Teilnehmern automatisch oder manuell zur Verfügung gestellt werden.
- Datensicherung durchführen
  Die bisherigen Änderungen an OpenScape Business müssen gesichert werden. Die Sicherung kann als Backup-Set z. B. auf einem USB-Medium oder im internen Netz gespeichert werden.
  Bei der UC Booster Card reicht es, eine Datensicherung des Kommunikationssystems durchzuführen. Bei dem UC Booster Server müssen die Daten

des Kommunikationssystems und separat die Daten der Kommunikationssoftware des UC Booster Servers gesichert werden.

6.7 Deinstallation der Kommunikationssoftware

Die Deinstallation der Kommunikationssoftware ist über eine Text-Konsole möglich.

6.7.1 Wie Sie die Kommunikationssoftware deinstallieren

Schritt für Schritt

1) Öffnen Sie ein Terminal (z. B. GNOME Terminal).

2) Geben Sie in der Shell-Oberfläche den Befehl `su` (für superuser = root) ein und bestätigen Sie mit der Eingabetaste.

3) Geben Sie in der Shell-Oberfläche das Passwort für den Benutzer "root" ein und bestätigen Sie mit der Eingabetaste.

4) Geben Sie in der Shell-Oberfläche den Befehl `oso_deinstall.sh` ein und bestätigen Sie mit der Eingabetaste. Folgen Sie den Anweisungen des Deinstallationsprogramms.

6.8 Hochrüstung von UC Booster Card auf UC Booster Server

Um ein OpenScape Business Kommunikationssystem mit integrierter UC Booster Card auf ein OpenScape Business Kommunikationssystem mit angeschlossenem UC Booster Server hochzurüsten, sind die nachstehend beschriebenen Schritte durchzuführen.

Hochrüst-Schritte

Führen Sie folgende Schritte der Reihe nach durch:

1. **Sicherung der Konfigurationsdaten**
   Führen Sie eine Sicherung der Konfigurationsdaten des Kommunikationssystems durch.
   Beschreibung der Datensicherung siehe *Sicherung der Konfigurationsdaten des Kommunikationssystems*.
2. **Änderung der IP-Adresse der UC Booster Card**
   Ändern Sie im WBM des Kommunikationssystems mit dem Wizard **Erstinstallation** die IP-Adresse der UC Booster Card in eine nicht benutzte IP-Adresse. Die Verbindung zu den UC Suite Clients wird getrennt.
   Beschreibung der IP-Adressänderung siehe *Systemeinstellungen*.

3. **Änderung der Applikationsauswahl**
   Ändern Sie im WBM des Kommunikationssystems mit dem Wizard **Erstinstallation** die Applikationsauswahl von **Paket mit UC Suite** auf **Paket mit UC Suite auf OSBiz UC Booster Server** und geben Sie als IP-Adresse des UC Booster Servers die ehemalige IP-Adresse der UC Booster Card an.
   Beschreibung der Applikationsauswahl siehe *UC-Lösung*.
4. **Installation des Linux-Servers**
   Auf dem Linux-Server ist das für den UC Booster Server freigegebene Linux-Betriebssystem zu installieren.
   Beschreibung der Linux-Installation siehe OpenScape Business Linux-Server Installationsanleitung.
5. **Änderung der IP-Adresse des UC Booster Servers**
   Für die IP-Adresse des UC Booster Servers (= IP-Adresse des Linux-Servers) muss die ehemalige IP-Adresse der UC Booster Card angegeben werden. Die IP-Adresse des Linux-Servers können Sie während der Installation des Linux-Betriebssystems eingeben oder nachträglich über YaST ändern.
   Beschreibung der IP-Adressvergabe während der Linux-Installation siehe OpenScape Business Linux-Server Installationsanleitung.
6. **Installation der Kommunikationssoftware**
   Auf dem Linux-Server ist die OpenScape Business Kommunikationssoftware zu installieren.
   Beschreibung der Installation der Kommunikationssoftware siehe *Installation der Kommunikationssoftware*.
7. **Konfiguration des UC Booster Servers**
   Geben Sie im WBM des UC Booster Servers die IP-Adresse des Kommunikationssystems ein.
   Beschreibung der IP-Adressvergabe des Kommunikationssystems siehe *Konfiguration des UC Booster Servers*.
8. **Neustart der Kommunikationssoftware**
   Führen Sie im WBM des UC Booster Servers einen Neustart der Kommunikationssoftware des UC Booster Servers durch.
   Beschreibung des Neustarts siehe *Restart (Neustart) der UC Applikation*.
9. **Update der Software**
   Die Software des Kommunikationssystems und des UC Booster Servers müssen auf den gleichen Software-Stand gebracht werden.
   Beschreibung des Software-Update siehe *Update*.
10. **Wiederherstellung der Konfigurationsdaten**
    Spielen Sie im WBM des Kommunikationssystems die Sicherung der Konfigurationsdaten des Kommunikationssystems ein. Kommunikationssystem und Kommunikationssoftware führen anschließend einen Neustart durch. Die Verbindung zu den UC Suite Clients ist wieder hergestellt.
    Beschreibung der Datenwiederherstellung siehe *Wiederherstellen*.

6.9 Verwendete Ports

Die OpenScape Business Systemkomponenten nutzen verschiedene Ports, die bei Bedarf in der Firewall freigeschaltet werden müssen. Für die Ports der Webbased Clients (z. B. myPortal to go) muss ein Port Forwarding im Router eingerichtet werden.

INFO: Die in der u.a. Liste mit "O" gekennzeichneten Ports sind optional, d.h. sie sind nicht dauerhaft in der Firewall geöffnet (z. B. ist der TFTP-Port nur bei aktiviertem Gate View offen).

Beschreibung	TCP	UDP	Portnummer	OpenScape Business X	UC Booster Card	OpenScape Business S	UC Booster Server
Systemkomponenten							
Admin Portal (https)	X		443	X	X	X	X
CAR Update Registration	X		12061	X		X	
CAR Update Server	X		12063	X		X	
CLA	X		61740	O		O	O
CLA Auto Discovery		X	23232	X		X	X
CSTA Message Dispatcher (CMD)	X		8900		X	X	X
CSTA Protocol Handler (CPH)	X		7004	X		X	
CSTA Service Provider (CSP)	X		8800		X	X	X
DHCP		X	67	X			
DLI	X		18443	X		X	X
DLSC	X		8084	X		X	X
DNS	X	X	53	X			
FTP	X		21	O		O	
FTP Passive	X		40000:40040	O		O	
Gate View	X		8000:8010		O	O	O
HFA	X		4060	X		X	
HFA Secure	X		4061	X		X	
JSFT	X		8771		X	X	X
JSFT	X		8772		X	X	X
LAS Cloud Service	X		8602	X			
LDAP Server	X		389		X	X	X
Manager E	X		7000	X			

Beschreibung	TCP	UDP	Portnummer	OpenScape Business X	UC Booster Card	OpenScape Business S	UC Booster Server
MEB SIP	X		15060		X		X
NAT traversal (NAT-T)		X	4500	X			
NTP		X	123	X			
Openfire Admin (https)	X		9091		X	X	X
OSBiz Multisite	X		8778		X	X	X
OSBiz myReports (http)	X		8101		X	X	X
OSBiz Status Server	X		8808	X		X	X
OSBiz User Portal	X	X	8779		X	X	X
Postgres	X		5432	X	X	X	X
RTP		X	29100:30530	X	X	X	X
SIP (server)	X	X	5060	X		X	
SIP TLS SIPQ (server)	X		5061	X		X	
SIP TLS Subscriber (server)	X		5062	X		X	
SNMP (Get/Set)		X	161	X		X	
SNMP (Traps)		X	162	X		X	
SSDP	X		3011	X		X	X
TFTP		X	69		O	O	O
VSL	X		8770		X	X	X
Webadmin for Clients	X		8803	X	X	X	X
XMPP Connection Manager	X		5262		X	X	X
XMPP Server	X		5269		X	X	X
Webbased Clients							
Webbased Clients (http)	X		8801	X	X	X	X
Webbased Clients (https)	X		8802	X	X	X	X

INFO: Aus Sicherheitsgründen wird empfohlen für die Webbased Clients ausschließlich https zu verwenden und ein Port Forwarding von extern TCP/443 nach intern TCP/8802 einzurichten.

7 Lizenzierung

Das flexible Lizenzkonzept von OpenScape Business bietet dem Kunden die Möglichkeit, den Leistungsumfang über Lizenzen genau seinen Anforderungen anzupassen. Alle Kommunikationssysteme OpenScape Business X und OpenScape Business S unterliegen diesem Lizenzkonzept. Telefone, UC Clients, UC-Funktionen und systemweite Leistungsmerkmale können so nach individuellem Kundenbedarf freigeschaltet werden. Für alle OpenScape Business Kommunikationssysteme werden einheitliche Lizenzen verwendet.

Soll OpenScape Business zu einem späteren Zeitpunkt erweitert oder mit zusätzlichen Leistungsmerkmalen ausgestattet werden, ist dies jederzeit durch den Erwerb weiterer Lizenzen möglich.

Alle Lizenzen sind immer an die Basislizenz des Kommunikationssystems gebunden und erlauben die Nutzung der erworbenen Leistungsmerkmale für die zugeordnete Version von OpenScape Business.

Um besondere Leistungsmerkmale dem Kunden zum Test oder zum Kennenlernen zur Verfügung zu stellen, können Evaluierungslizenzen mit einer Laufzeit von 90 Tagen bestellt werden.

Activation Period

Die Activation Period wird durch den erstmaligen Zugriff auf das WBM gestartet. Nach der Erstinstallation des Kommunikationssystems muss innerhalb einer Zeitspanne von 30 Tagen (Activation Period) die Lizenzaktivierung vorgenommen werden. Das Produkt ist während der Activation Period voll funktionsfähig und die maximale Anzahl an Lizenzen steht zur Nutzung zur Verfügung.

Ist nach Ablauf der Activation Period keine Lizenzierung erfolgt, ist das Kommunikationssystem nur noch sehr eingeschränkt nutzbar. Eine interne Kommunikation zwischen den Teilnehmern ist möglich, aber nach extern können nur die beiden ersten aktiven Telefone telefonieren (z. B. für Notrufe). Der Zugang zum Kommunikationssystem über die Fernverwaltung (Remote-Zugang) ist weiterhin möglich. Das System befindet sich ebenfalls in diesem eingeschränkt nutzbaren Zustand, wenn die Erstinstallation nur mit dem Manager E durchgeführt wurde, da hierüber die Activation Period nicht gestartet wird.

Struktur der Lizenzen

Die Lizenzen für das Kommunikationssystem sind folgendermaßen strukturiert:

- eine Basislizenz aktiviert die Software des Kommunikationssystems dauerhaft und ist Voraussetzung für die Aktivierung aller weiteren Lizenzen.
- Teilnehmer-Lizenzen zur Aktivierung der Telefone für die externe Sprachkommunikation.
- User-orientierte Lizenzen zum Freischalten spezifischer Leistungsmerkmale für die Benutzer.
- Systemlizenzen um allgemeine Leistungsmerkmale systemweit freizuschalten.

Migration

Für bestehende HiPath 3000 V9 Kunden wird eine Lizenzmigration über eine Upgradelizenz angeboten. Die Lizenzmigration bietet Investitionsschutz für den Kunden für die weitere Nutzung der Telefone und der Sprachleistungsmerkmale.

7.1 Lizenzierungsverfahren

Für die Lizenzierung steht mit dem OpenScape Lizenz-Management ein zentralisiertes Verfahren zur Verwaltung und Aktivierung von Lizenzen zur Verfügung. Dieses stellt sicher, dass ein Kunde jeweils genau den Systemausbau bzw. diejenigen Leistungsmerkmale verwenden kann, für die er die entsprechenden Lizenzen (Nutzungsrechte) erworben hat.

Die Lizenzen der OpenScape Business Kommunikationssysteme werden an die Locking ID bzw. die Advanced Locking ID des Kommunikationssystems gebunden (siehe *Locking ID und Advanced Locking ID*).

Der Kunde bestellt die gewünschten Leistungsmerkmale und erhält einen Lizenzaktivierungsschlüssel (LAC). Nach erfolgreicher Erstinstallation des Kommunikationssystems aktiviert der Kunde die erworbenen Lizenzen mit Hilfe einer Lizenzdatei. Die Lizenzdatei stellt dem System einen Lizenzpool mit allen erworbenen Lizenzen für die anschließende Lizenzzuordnung zur Verfügung.

Das WBM bietet Wizard-gesteuert die Funktionen für die Kunden-Registrierung, die Lizenzaktivierung und die Lizenzzuordnung für Standalone-Systeme und Systeme in einem OpenScape Business Netzverbund an. Eine Lizenzierung mit dem Manager E ist nicht möglich.

Schritte zur erfolgreichen Lizenzierung

1. Konfiguration des Systems innerhalb der Activation Period
2. Registrierung der Kundendaten
3. Lizenzaktivierung
4. Lizenzzuordnung

Kunden-Registrierung

Im Rahmen der Lizenzierung sind für die Registrierung des Kunden die Kundendaten des jeweiligen Systems zwingend einzugeben. Die Kundendaten werden verwendet, um im Fall von sicherheitsrelevanten Sachverhalten, insbesondere Produktrückrufen schnell informieren zu können. Zusätzlich erhalten die Kunden Informationen zur Vermeidung von Lizenzmissbrauch durch Dritte, z. B. über die Neuverknüpfung der Lizenzinformationen.

Lizenzaktivierung

Bei der Lizenzaktivierung werden über die Lizenzverwaltung des WBM die erworbenen Lizenzen an das Kommunikationssystem gebunden. Dafür stehen 2 Methoden zur Verfügung:

- Online-Aktivierung
  Bei der Online-Aktivierung wird nach Eingabe des LAC über das Internet eine Verbindung zum zentralen Lizenzserver (Central License Server, CLS) hergestellt und die Lizenzdatei automatisch an den im Kommunikationssystem integrierten Lizenzagenten (Customer License Agent, CLA) übertragen. Anschließend werden die Lizenzen automatisch aktiviert.
- Offline-Aktivierung
  Bei der Offline-Aktivierung besteht keine Verbindung des Kommunikationssystems zum zentralen Lizenzserver (Central License Server, CLS). Die Lizenzdatei wird von einem autorisierten Partner am CLS generiert und muss während der Lizenzaktivierung manuell an den im Kommunikationssystem integrierten Lizenzagenten (Customer License Agent, CLA) übertragen werden.

Lizenzzuordnung

Alle erworbenen Lizenzen werden über die Lizenzverwaltung des WBM den Teilnehmern fest zugeordnet.

Um Teilnehmern Lizenzen zuordnen zu können, müssen die Teilnehmer zuerst mit dem WBM eingerichtet werden, z. B. bei der Erstinstallation. Jede Systemkonfiguration kann unabhängig von den vorhandenen Lizenzen eingerichtet werden. Erst mit der Lizenzzuordnung kann das entsprechende Leistungsmerkmal genutzt werden.

Bei der Lizenzzuordnung wird zwischen Konfiguration und Vergabe von Lizenzen unterschieden. Für Teilnehmer und User-orientierte Lizenzen werden Lizenzanforderungen konfiguriert. Ist für eine Lizenzanforderung eine Lizenz in dem Lizenzpool vorhanden, wird das entsprechende Leistungsmerkmal freigeschaltet. Ist keine Lizenz in dem Lizenzpool vorhanden, bleibt die konfigurierte Lizenzanforderung erhalten, aber das entsprechende Leistungsmerkmal ist nicht freigeschaltet. Bei Bedarf müssen fehlende Lizenzen nachgekauft werden.

Lizenzierung im Netzverbund

Für einen OpenScape Business Netzverbund wird eine netzweite Lizenzdatei (Netzwerklizenzdatei) von einem autorisierten Partner am zentralen Lizenzserver (CLS) generiert. Diese netzweite Lizenzdatei wird vom zentralen Lizenzagenten (CLA) des Master-Knoten verwaltet und stellt den einzelnen Knoten die Lizenzen zur Verfügung. Die Zuordnung der Lizenzen erfolgt über das WBM jedes einzelnen Knotens. Innerhalb eines Netzverbunds können die Lizenzen über das WBM verschoben werden.

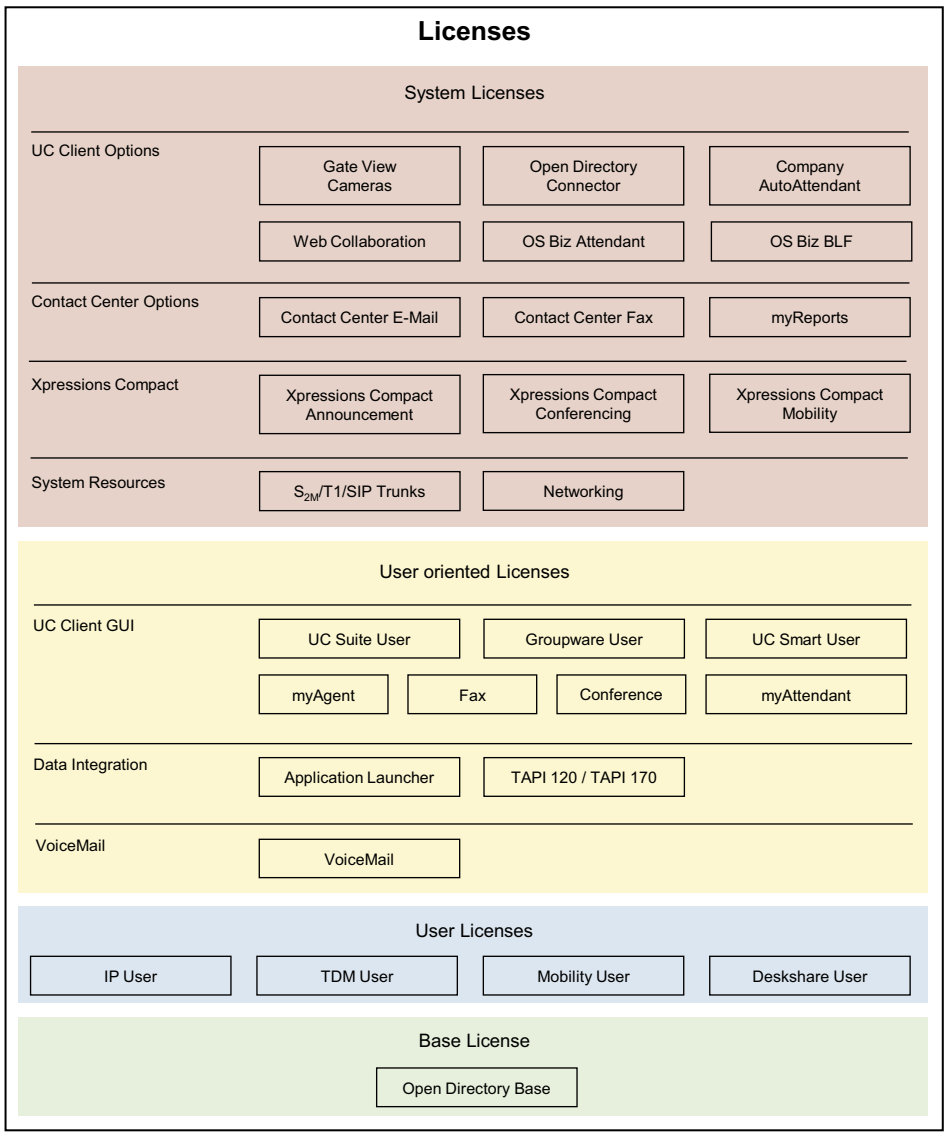
Bei der Lizenzierung eines Netzverbunds ist eine Online-Aktivierung nicht möglich.

7.2 Lizenzen

Um die Leistungsmerkmale des Kommunikationssystems nutzen zu können, sind Lizenzen zu erwerben. Innerhalb einer gewissen Zeitspanne (Activation Period) müssen die erworbenen Lizenzen aktiviert werden.

Die Lizenzen sind thematisch zu Lizenzgruppen zusammengefasst. Folgende Lizenzgruppen stehen zur Verfügung:

- Basislizenzen
- Teilnehmer-Lizenzen
- User-orientierte Lizenzen
- Systemlizenzen



Die o.a. Lizenzen können für OpenScape Business X, OpenScape Business S und OpenScape Business UC Booster Server verwendet werden. Der UC Booster Server hat keine eigene Basislizenz. Die Lizenzen decken alle Leistungsmerkmale ab und können nach den Wünschen des Kunden zusammengestellt werden. Die Kombinationsmöglichkeiten der Lizenzen werden bei der Lizenz- und Lizenzprofilzuordnung genauer erklärt.

Teilnehmer-Lizenzen und User-orientierte Lizenzen werden den Teilnehmern fest zugeordnet.

7.2.1 Basislizenz

Die Basislizenz erlaubt die generelle Nutzung des Kommunikationssystems und ist Voraussetzung für die Aktivierung aller weiteren Lizenzen.

Internet-Telefonie und Notbetrieb ist auch ohne Basislizenz möglich.

Folgende Basislizenzen steht zur Verfügung:

- **OpenScape Business V1 X1 Base**
  für die Freischaltung des V1-Funktionsumfangs von
  – OpenScape Business X1
  Die Basislizenz enthält zusätzlich die Lizenz OpenDirectory Base für die Nutzung von Open Directory Service (ODS). Damit kann die UC-Lösung UC Smart mit einer externen Datenbank verbunden werden.
- **OpenScape Business V1 Base**
  für die Freischaltung des V1-Funktionsumfangs von
  – OpenScape Business X3/X5/X8 mit oder ohne UC Booster (UC Booster Card oder UC Booster Server) oder
  – OpenScape Business S
  Die Basislizenz enthält zusätzlich die Lizenz OpenDirectory Base für die Nutzung von Open Directory Service (ODS). Damit können die UC-Lösungen UC Suite oder UC Smart mit einer externen Datenbank verbunden werden.

7.2.2 Teilnehmer-Lizenzen

Jeder am Kommunikationssystem angeschlossene Teilnehmer benötigt für die externe Telefonie eine Teilnehmer-Lizenz. Diese Lizenz wird der Rufnummer des Teilnehmers über das WBM fest zugeordnet.

Die Teilnehmer-Lizenzen beinhalten die umfangreiche Sprachfunktionälität von OpenScape Business. Für die Nutzung der UC-Lösungen UC Smart oder UC Suite sind weitere Lizenzen nötig (siehe *User-orientierte Lizenzen*).

Folgende Teilnehmer-Lizenzen stehen zur Verfügung:

- **IP User**
  für die Nutzung von IP-Systemtelefonen (HFA) und SIP-Telefonen.
- **TDM User**
  für die Nutzung von UP0-Systemtelefonen, analogen Telefonen, analogem FAX, ISDN-Telefonen, ISDN-Fax und DECT-Telefonen.
- **Mobility User**
  für die Nutzung von GSM-/Mobiltelefonen, Smartphones und Tablet-PCs als Nebenstelle des Kommunikationssystems. Für die Nutzung von myPortal for Mobile/Tablet, myPortal to go und Mobility Entry. Die Zuordnung eines zusätzlichen Tischtelefons ist nicht erforderlich.

- **DeskShare User**
  für die Nutzung des Leistungsmerkmals DeskSharing. Diesem Teilnehmer ist nur eine Rufnummer und kein physikalisches Telefon fest zugeordnet. Der Teilnehmer kann bestimmte IP-Systemtelefone unter seiner eigenen Rufnummer nutzen und hat an den Telefonen Zugriff auf seine persönlichen Telefoneinstellungen.

Flexible Teilnehmer-Lizenzierung

Mit der flexiblen Teilnehmer-Lizenzierung können TDM-, Mobility- und DeskShare User auch mit IP User Lizenzen lizenziert werden. Sind alle erworbenen TDM-, DeskShare- und Mobility User Lizenzen den Teilnehmern zugeordnet und besteht Bedarf für weitere TDM-, DeskShare- und Mobility User, können übrige IP User Lizenzen verwendet werden, um diesen Bedarf zu decken.

Voraussetzung für die Nutzung der flexiblen Teilnehmer-Lizenzierung ist die Software-Version V1R3.3 und eine am CLS neu generierte Lizenzdatei, die in die OpenScape Business eingespielt und aktiviert werden muss.

Verwandte Themen

- Lizenzzuordnung (Standalone)

7.2.3 User-orientierte Lizenzen

User-orientierte Lizenzen sind teilnehmerbezogen und berechtigen zur Nutzung der Unified Communications Leistungsmerkmale und der Applikationen zur Datenintegration. Eine User-orientierte Lizenz setzt immer eine Teilnehmer-Lizenz voraus und ist der Rufnummer des Teilnehmers fest zugeordnet.

Folgende User-orientierte Lizenzen stehen zur Verfügung:

VoiceMail

- **VoiceMail**
  für die Nutzung einer persönlichen Sprachbox (VoiceMail) über das Telefon (TUI) und über die Oberfläche der UC-Lösungen UC Smart oder UC Suite.

> ***INFO:*** Wird die UC-Lösung UC Smart auf UC Suite erweitert, bleiben die vorhandenen VoiceMail-Lizenzen und die Zuordnung zu den Teilnehmern erhalten.

UC Client Benutzer-Oberfläche

- **UC Smart User**
  für die Nutzung der UC Smart Funktionen der Communications Clients myPortal Smart, myPortal to go, myPortal for Mobile/Tablet, Application Launcher und weiteren Web Services Clients.

- **UC Suite User**
  für die Nutzung der UC Suite Funktionen der Communications Clients myPortal for Desktop, myPortal to go, myPortal for Mobile/Tablet, Application Launcher und weiteren Web Services Clients.
- **Groupware User**
  für die Nutzung der UC Suite Funktionen der Communications Clients myPortal for Outlook, myPortal to go, myPortal for Mobile/Tablet, Application Launcher und weiteren Web Services Clients.
- **Fax**
  für die Nutzung einer Faxbox innerhalb der UC Suite. Voraussetzung ist zusätzlich eine UC Suite User oder eine Groupware User Lizenz.
- **Conference**
  für die Nutzung der Konferenz-Verwaltung innerhalb der UC Suite, wie z. B. Verwalten und Einleiten von permanenten und wiederkehrenden Konferenzen. Voraussetzung ist zusätzlich eine UC Suite User Lizenz oder eine Groupware User Lizenz.
  Für die Teilnahme an Konferenzen wird keine Lizenz benötigt.
- **myAttendant**
  für die Nutzung der UC Suite Vermittlungsfunktionen.
- **myAgent**
  für die Nutzung der Contact Center Funktionen, wie z. B. Informationen zu Warteschlangen, Popups mit Kundeninformationen bei ankommenden Anrufen, Zugriff auf die Anrufhistorie.
- **Upgrade von myPortal Smart auf myPortal for Desktop**
  für den Upgrade des UC Clients myPortal Smart auf den UC Client myPortal for Desktop zur Nutzung der vollen UC-Funktionalität wie z. B. Konferenz und Fax.

INFO: Für die Mobile Clients myPortal for Mobile/Tablet und myPortal to go wird zusätzlich zur Mobility User Lizenz für die UC-Lösung UC Smart eine UC Smart User Lizenz und für die UC-Lösung UC Suite eine UC Suite User Lizenz bzw. eine Groupware User Lizenz benötigt.

Datenintegration

- **Application Launcher**
  für die anrufbezogene Steuerung von Applikationen auf einem Client-PC bei ankommenden und gehenden Anrufen, z. B. Aufruf einer Applikation oder Anzeige von Anruferdaten. Der Application Launcher kann mit UC Smart oder UC Suite betrieben werden und benötigt zusätzlich eine UC Smart User Lizenz (bei UC Smart) oder eine UC Suite User / Groupware User Lizenz (bei UC Suite). Optional kann er den Open Directory Service nutzen.
- **OpenScape Business TAPI**
  für die Nutzung von TAPI-konformen Applikationen und PC-unterstütztes Telefonieren mit kundeneigenen Programmen verschiedener Software-Hersteller. Voraussetzung ist UC Booster (UC Booster Card oder UC Booster Server).

7.2.4 Systemlizenzen

Systemlizenzen sind nicht teilnehmerbezogen und schalten die systemweiten Leistungsmerkmale frei. Diese Leistungsmerkmale können von allen Teilnehmern des Kommunikationssystems genutzt werden.

Folgende Systemlizenzen stehen zur Verfügung.

System Ressourcen

- **S_{2M}/T1/SIP Trunks**
  für die Nutzung von S_{2M}-/T1- und ITSP-Kanälen. S_0-Kanäle müssen nicht lizenziert werden, dazu zählen auch Anschaltungen zu S_0-Fax-Servern im PP-Modus. Bei Primärmutiplex-Verbindungen S_{2M} oder T1 (USA) werden die einzelnen Sprachkanäle lizenziert. Bei ITSP-Verbindungen wird die Anzahl der gleichzeitigen Verbindungen zu einem oder mehreren ITSP-Providern (SIP-Providern) lizenziert. Die Anzahl der möglichen gleichzeitigen Verbindungen ist abhängig von der Bandbreite des Anschlusses.
- **Networking**
  für die IP-Vernetzung via SIP-Q/native SIP und/oder die TDM-Vernetzung via CorNet-NQ oder QSIG. Für die Vernetzung der UC Suite Applikationen. Pro Knoten wird eine Lizenz benötigt.

> ***INFO:*** Die Networking-Lizenz schaltet für einen Knoten die Leitungen für die Sprachvernetzung und die UC Suite Vernetzung frei. Für Vernetzungsleitungen werden keine S_{2M}/T1/SIP Trunk Lizenzen benötigt.

Tabelle: Übersicht über die System Ressourcen Lizenzen (S2M/ITSP)

Protokoll	Lizenzen			
	keine Lizenz	OSBiz Networking (1x pro System)	OSBiz S2M / ITSP (1x pro Kanal)	TDM-User
S0 intern				
Fax-Server (DSS1/QSIG)	X			
Euro-Bus				pro S0-Teilnehmer
S0-Amtsleitungen				
Euro-Amt PP	X			
Euro-Amt PMP	X			
S2M-Amtsleitungen				
Euro-Amt PP			X	
ITSP-Provider				
ITSP 1 bis 4			X	
S0-Vernetzung				

Protokoll	Lizenzen			
	keine Lizenz	OSBiz Networking (1x pro System)	OSBiz S2M / ITSP (1x pro Kanal)	TDM-User
QSIG		X		
CorNet-NQ		X		
S2M-Vernetzung				
QSIG		X		
CorNet-NQ		X		
SIP-Vernetzung				
SIP-Q		X		
native SIP		X		

Xpressions Compact

- **Xpression Compact Announcement**
  für die Nutzung der Xpressions Compact Ansagen-Funktionen, wie z. B. das Aufzeichnen von speziellen Ansagen für Informations- oder Vermittlungsmailboxen. Pro Xpressions Compact ist eine Lizenz nötig.
- **Xpression Compact Conferencing**
  für die Nutzung der Xpressions Compact Konferenz-Funktionen, wie z: B. das Verwalten und Ausführen von Konferenzen, Steuerung der Konferenzen über einen Web-Client. Pro Xpressions Compact können 3 Lizenzen erworben werden.
- **Xpression Compact Mobility**
  für die Nutzung der Xpressions Compact Mobility-Funktionen, wie z. B. den One Number Service (Teilnehmer ist für alle Gespräche über jedes ihm zugeordnete Telefon mit einer Rufnummer erreichbar). Pro Xpressions Compact können 6 Lizenzen erworben werden.

Contact Center Optionen

- **Contact Center Mail**
  für die Einrichtung von einer oder mehreren E-Mail-Boxen für das Empfangen und Senden von E-Mails für Contact-Center-Agenten. Voraussetzung ist eine Teilnehmer-Lizenz und eine myAgent Lizenz. Pro Knoten ist eine Lizenz nötig.
- **Contact Center Fax**
  für die Einrichtung von einer oder mehreren Faxboxen für das Empfangen und Senden von Faxen für Contact-Center-Agenten. Voraussetzung ist eine Teilnehmer-Lizenz und eine myAgent Lizenz. Pro Knoten ist eine Lizenz nötig.
- **myReports**
  für die Erstellung von Statistiken über die Auslastung der Contact Center-Ressourcen nach unterschiedlichen Kriterien. Mit dem Schedule Manager können aus über 100 vordefinierten Berichtsvorlagen für Telefon-, E-Mail- und Fax-Kontakte Berichte erstellt werden. Die Verwaltung der Berichtsvor-

lagen erfolgt über den Report Manager mit der Möglichkeit zur Umgruppierung sowie zum Hinzufügen und Löschen neu erstellter Report-Vorlagen.

UC Client Optionen

- **Web Collaboration**
  für die Einbindung der Web Collaboration in die UC Suite. Voraussetzung ist das Produkt OpenScape Web Collaboration V7. Pro Knoten ist eine Lizenz nötig.

  INFO: OpenScape Web Collaboration ist eine skalierbare und sichere multimediale Webkonferenzlösung. Sie kann kontextbezogen gestartet werden aus applikationsgesteuerten Konferenzen, Systemkonferenzen über das Telefon und Zweier-Gesprächen über PopUp-Fenster.

- **Open Directory Connector**
  für die Verbindung zum Open Directory Service (ODS), um auf eine externe Datenbank oder ein externes Verzeichnis zugreifen zu können. Pro Knoten können bis zu vier Datenbanken angebunden werden.
- **Company AutoAttendant**
  für die Nutzung eines zentralen, UC Smart oder UC Suite basierten AutoAttendant zur automatischen Vermittlung von Gesprächen. Pro Knoten ist eine Lizenz nötig.
  Ansagen vom Typ "Wartemusik" (endlos) werden nur mit dieser Lizenz abgespielt.
- **Gate View Cameras**
  für Videoüberwachung, die in Echtzeit Videobilder auf Ihrem OpenStage Telefon, einem PC oder einem Smartphone bereitstellt. Für jede der 8 möglichen Kameras innerhalb eines Knotens ist eine eigene Lizenz nötig.
- **OpenScape Business Attendant**
  für die Nutzung des PC-Vermittlungsplatzes OpenScape Business Attendant. Pro Knoten können bis zu 8 OpenScape Business Attendant lizenziert werden.
  Soll OpenScape Business Attendant auch Zugriff auf Präsenz-Informationen haben, ist zusätzlich eine UC Smart oder UC Suite User Lizenz nötig.
- **OpenScape Business BLF**
  für die Nutzung der zusätzlichen Besetztlampenfeldanzeige OpenScape Business BLF. Pro Teilnehmer ist eine BLF-Lizenz und eine UC-Smart- oder UC-Suite User Lizenz erforderlich. Pro Knoten können bis zu 50 OpenScape Business BLF lizenziert werden.

Für die netzweite Bereitstellung von Präsenz- und BLF-Information ist zusätzlich zu OpenScape Business Attendant und BLF ein BLF-Server erforderlich. Der BLF-Server benötigt je Knoten eine IP User Lizenz und eine UC-Smart oder UC-Suite User Lizenz.

7.2.5 Evaluierungslizenzen

Mit einer Evaluierungslizenz können besondere Leistungsmerkmale über einen bestimmten Zeitraum (Evaluation Period) mit vollem Leistungsumfang kostenlos getestet werden. Wird während der Evaluation Period eine reguläre Lizenz für das Leistungsmerkmal aktiviert, wird die Evaluierungslizenz deaktiviert.

Folgende Evaluierungslizenzen stehen zur Verfügung:

- **OpenScape Business V1 UC Smart / UC Suite Evaluierung**
  Diese Evaluierungslizenz ist für Kunden bestimmt, die die UC-Funktionen von UC Smart oder UC Suite testen möchten. Mit dieser Evaluierungslizenz können alle Leistungsmerkmale von UC Smart oder UC Suite genutzt werden.

  INFO: Diese Evaluierungslizenz ist nicht einsetzbar, falls sich das Kommunikationssystem in einem Netzverbund befindet und die Lizenz "Networking" aktiv ist. Sind bereits Voicemail Lizenzen vorhanden, werden diese in Kombination mit den neuen UC Evaluierungslizenzen verwendet.

- **OpenScape Business V1 UC Suite Contact Center Evaluierung**
  Diese Evaluierungslizenz ist für Kunden bestimmt, die das Multimedia Contact Center testen möchten. Mit dieser Evaluierungslizenz können alle Leistungsmerkmale des Multimedia Contact Centers genutzt werden.

  INFO: Wird das Multimedia Contact Center nicht innerhalb der Evaluation Period lizenziert, muss der Administrator vor Ablauf der Evaluierungslizenz die Einstellungen am Contact Center wieder rückgängig machen (z. B. Zeitpläne und Warteschlangen löschen, Agenten deaktivieren, usw.), da es sonst zu Fehlverhalten bei OpenScape Business kommen kann.

- **OpenScape Business V1 CRM Evaluierung**
  Diese Evaluierungslizenz ist für Kunden bestimmt, Application Launcher, Open Directory Service und TAPI testen möchten.
- **OpenScape Business V1 Attendant Evaluierung**
  Diese Evaluierungslizenz ist für Kunden bestimmt, die die Applikation OpenScape Business Attendant testen möchten.
- **OpenScape Business V1 BLF Evaluierung**
  Diese Evaluierungslizenz ist für Kunden bestimmt, die die Applikation OpenScape Business BLF testen möchten, z. B. für die eigenständige Anzeige von Besetztlampenfeld- und Präsenz-Informationen.

Regeln

- Die Aktivierung einer Evaluierungslizenz erfolgt am Customer License Server (CLS) und ist nur einmal möglich.
- Die Evaluation Period beträgt 90 Tage. Nach 60 Tagen wird im Display der Systemtelefone die verbleibende Zeit in Tagen rückwärts gezählt.

- Nach Ablauf der Evaluation Period erfolgt die automatische Deaktivierung des Leistungsmerkmals.
- Evaluierungslizenzen können gleichzeitig im System aktiv sein, enden dann aber zu unterschiedlichen Zeiten.
- Ist eine zeitlich unbefristete Lizenz aktiv, wird die Evaluierungslizenz nicht gestartet oder, falls bereits vorhanden, gestoppt.

7.2.6 Migrations-Lizenzen

Migrations-Lizenzen sind nötig, um von einem HiPath 3000 Kommunikationssystem oder einem OpenScape Office V3 Softswitch auf OpenScape Business V1 hochzurüsten.

Die Lizenzmigration von HiPath 3000 Systemen setzt ein laufendes und ggf. lizenziertes HiPath 3000 V9 System voraus. Die Schritte zur Hardware- und Lizenzmigration sind genau zu beachten (siehe *Migration*). Reine HiPath 3000 TDM Systeme ohne Lizenzen sind zuerst auf Version 9 hochzurüsten und können anschließend mit einer Migrations-Lizenz auf OpenScape Business hochgerüstet werden. Für die Lizenzmigration von OpenScape Office V3 LX (Softswitch) wird eine separate Migrations-Lizenz auf OpenScape Business S benötigt.

Folgende Migrations-Lizenzen stehen zur Verfügung:

- **HiPath 3000 V9 Upgrade auf OpenScape Business V1**
  für die Migration von HiPath 3000 V9 auf OpenScape Business X3/X5/X8.
- **HiPath 3000 V8 Upgrade auf OpenScape Business V1**
  für die Migration von HiPath 3000 V8 auf HiPath 3000 V9 und anschließend auf OpenScape Business V1.
- **HiPath 3000 V7 Upgrade auf OpenScape Business V1**
  für die Migration von HiPath 3000 V7 auf HiPath 3000 V9 und anschließend auf OpenScape Business V1.
- **OpenScape Office V3 LX Upgrade auf OpenScape Business V1 S**
  für die Softswitch-Migration von OpenScape Office V3 LX auf OpenScape Business S V1.

7.2.7 Vorschläge für Lizenzkombinationen

Lizenzen können beliebig kombiniert werden. Im Folgenden sind einige Vorschläge aufgelistet, wie Lizenzen sinvoll kombiniert werden können, um die gewünschten Funktionen zu nutzen.

Bitte beachten Sie, dass für manche Funktionen mehrere Lizenzen benötigt werden.

Telefonie

- Benötigt: Teilnehmer-Lizenz IP User oder TDM User oder DeskShare User

INFO: Ohne gültige Lizenz ist das Telefon nur für interne Verbindungen freigeschaltet.

Tefefonie mit UC Smart

- Telefonie mit Sprachbox (UC Smart)
  - Benötigt: Teilnehmer-Lizenz IP User oder TDM User oder DeskShare User
  - Benötigt: User-orientierte Lizenz VoiceMail

- Telefonie mit Mobility Entry (DISA basiertes Mobility)
  - Benötigt: Teilnehmer-Lizenz Mobility User

- Telefonie mit myPortal Smart
  - Benötigt: Teilnehmer-Lizenz IP User oder TDM User oder DeskShare User
  - Benötigt: User-orientierte Lizenz UC Smart User
  - Optional: User-orientierte Lizenz VoiceMail

- Telefonie mit myPortal to go
  - Benötigt: Teilnehmer-Lizenz Mobility User
    In der Betriebsart **Office-Benutzer** (Steuerung des Bürotelefons) ist keine Mobility User Lizenz notwendig.
  - Benötigt: User-orientierte Lizenz UC Smart User
  - Optional: User-orientierte Lizenz VoiceMail

- Telefonie mit myPortal for Mobile/Tablet
  - Benötigt: Teilnehmer-Lizenz Mobility User
  - Benötigt: User-orientierte Lizenz UC Smart User
  - Optional: User-orientierte Lizenz VoiceMail

- Telefonie mit optiClient Attendant
  - Benötigt: Teilnehmer-Lizenz IP User oder TDM User oder DeskShare User
  - Benötigt: Systemlizenz OpenScape Business Attendant
  - Optional: User-orientierte Lizenz VoiceMail
  - Optional: User-orientierte Lizenz UC Smart User (für Presence-Anzeige)

Telefonie mit UC Suite

- Telefonie mit Sprachbox (UC Suite)
  - Benötigt: Teilnehmer-Lizenz IP User oder TDM User oder DeskShare User

  - Benötigt: User orientierte Lizenz VoiceMail

- Telefonie mit myPortal for Desktop
  - Benötigt: Teilnehmer-Lizenz IP User oder TDM User oder DeskShare User
  - Benötigt: User-orientierte Lizenz UC Suite User
  - Optional: User-orientierte Lizenz VoiceMail
  - Optional: User-orientierte Lizenz Fax
  - Optional: User-orientierte Lizenz Conference
  - Optional: Systemlizenz Web Collaboration

- Telefonie mit myPortal for Outlook
  - Benötigt: Teilnehmer-Lizenz IP User oder TDM User oder DeskShare User
  - Benötigt: User-orientierte Lizenz Groupware User
  - Optional: User-orientierte Lizenz VoiceMail
  - Optional: User-orientierte Lizenz Fax
  - Optional: User-orientierte Lizenz Conference
  - Optional: Systemlizenz Web Collaboration

- Telefonie mit myPortal to go
  - Benötigt: Teilnehmer-Lizenz Mobility User
    In der Betriebsart **Office-Benutzer** (Steuerung des Bürotelefons) ist keine Mobility User Lizenz notwendig.
  - Benötigt: User-orientierte Lizenz UC Smart User
  - Optional: User-orientierte Lizenz VoiceMail

- Telefonie mit myPortal for Mobile/Tablet
  - Benötigt: Teilnehmer-Lizenz Mobility User
  - Benötigt: User-orientierte Lizenz UC Smart User
  - Optional: User-orientierte Lizenz VoiceMail

- Telefonie mit myAttendant
  - Benötigt: Teilnehmer-Lizenz IP User oder TDM User oder DeskShare User
  - Benötigt: User-orientierte Lizenz myAttendant
  - Optional: User-orientierte Lizenz VoiceMail

Nutzung des Contact Centers

- Benötigt: Teilnehmer-Lizenz IP User oder TDM User oder DeskShare User oder Mobility User
- Benötigt: User-orientierte Lizenz myAgent
- Optional: Systemlizenz Contact Center E-Mail

- Optional: Systemlizenz Contact Center Fax
- Optional: Systemlizenz myReports

Nutzung des Company AutoAttendant

- Benötigt: Systemlizenz Company AutoAttendant

7.3 Lizenzierung eines Kommunikationssystems (Standalone)

Die Lizenzierung eines Standalone-Systems ist in einer bestimmten Reihenfolge durchzuführen. Diese Reihenfolge ist am Beispiel eines der Kommunikationssysteme OpenScape Business X dargestellt.

Wie Sie Schritt 3 und Schritt 4 mit Hilfe des WBM durchführen, ist in den nachfolgenden Unterkapiteln beschrieben.

1. **Lizenz-Autorisierungscode (LAC)**
   Der Kunde erhält beim Kauf von Lizenzen einen Lizenz-Autorisierungscode (LAC). Die Daten über die erworbenen Lizenzen sind in der Datenbank des zentralen Lizenzservers (CLS) gespeichert.
2. **Installation und Konfiguration**
   Der Kunde oder Servicetechniker installiert und konfiguriert das Kommunikationssystem mit Hilfe der WBM-Wizards (u.a. Teilnehmer und Leitungen). Beim ersten Starten des WBM ist das aktuelle Datum einzugeben. Ab diesem Zeitpunkt startet die Activation Period (Zeitspanne von 30 Tagen, in der die Lizenzierung des Kommunikationssystems vorgenommen werden muss).
3. **Lizenzaktivierung**
   Der Kunde oder Servicetechniker aktiviert die Lizenzen mit dem WBM entweder online über den Lizenz-Autorisierungscode (Online-Lizenzaktivierung) oder offline direkt über die Lizenzdatei (Offline-Lizenzaktivierung).
4. **Lizenzzuordnung**
   Der Kunde oder Servicetechniker ordnet mit dem WBM den Teilnehmern und den Leitungen die erworbenen Lizenzen zu. Nach erfolgreicher Zuordnung werden die lizenzierten Leistungsmerkmale freigeschaltet.

Verwandte Themen

- Lizenzaktivierung (Standalone)
- Lizenzzuordnung (Standalone)

7.3.1 Lizenzaktivierung (Standalone)

Nachdem ein Produkt oder ein Leistungsmerkmal erworben wurde, müssen zuerst die mit dem Produkt/Leistungsmerkmal bereitgestellten Lizenzen aktiviert werden. Nach erfolgreicher Aktivierung erfolgt dann die Lizenzzuordnung.

Um die Lizenzen zu aktivieren gibt es zwei Möglichkeiten:

- **Online-Lizenzaktivierung** (über den Lizenz-Autorisierungscode)
  Der Kunde oder Servicetechniker überträgt mit Hilfe des WBM den Lizenz-Autorisierungscode via Internet an den zentralen Lizenzserver (CLS). Zusammen mit dem LAC wird die Locking ID des Kommunikationssystems für die Lizenzaktivierung verwendet. Der CLS erzeugt aus den Daten eine Lizenzdatei und schickt diese zurück an das System, das daraufhin die erworbenen Lizenzen aktiviert.
  Für den Zugang zum CLS benötigen Sie eine Internet-Verbindung. Die IP-Adresse des CLS ist im WBM unter **Lizenzverwaltung > Einstellungen** hinterlegt und kann falls nötig vom Administrator mit Profil **Expert** geändert werden.

  INFO: Für die Online-Lizenzaktivierung wird standardmäßig der Port 7790 verwendet. Dieser Port muss in der Firewall des Kundennetzes freigegeben sein.

  INFO: Bevor die Online-Lizenzierung durchgeführt werden kann, müssen zuerst die Registrierungsdaten korrekt erfasst werden.

- **Offline-Lizenzaktivierung** (direkt über die Lizenzdatei)
  Der Kunde oder Servicetechniker meldet sich am zentralen Lizenzserver (CLS) an und gibt dort den Lizenz-Autorisierungscode zusammen mit der Locking ID des Kommunikationssystems ein. Der CLS erzeugt aus den Daten eine Lizenzdatei. Der Kunde oder Servicetechniker lädt sich die Lizenzdatei herunter und spielt diese in das WBM ein. Das System aktiviert daraufhin die erworbenen Lizenzen.
  Die IP-Adresse des CLS ist im WBM unter **Lizenzverwaltung > Einstellungen** hinterlegt und kann falls nötig vom Administrator mit Profil **Expert** geändert werden.

Wenn das Kommunikationssystem erweitert werden soll, können weitere Lizenzen zugekauft werden. Beim Erwerb zusätzlicher Lizenzen wird ein weiterer Lizenz-Autorisierungscode (LAC) ausgeliefert, mit dem die neu erworbenen Lizenzen aktiviert werden können.

INFO: Zusätzlich erworbene Lizenzen können auch über Remote aktiviert werden.

Verwandte Themen

- Lizenzzuordnung (Standalone)
- Lizenzierung eines Kommunikationssystems (Standalone)

7.3.1.1 Wie Sie Lizenzen online aktivieren (Standalone)

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.
- Sie kennen den LAC (Lizenz-Autorisierungscode) für die Lizenzfreischaltung.
- Für die Verbindung zum Lizenzserver muss das Kommunikationssystem eine Verbindung zum Internet haben.



Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.

2) Klicken Sie im Navigationsbaum auf **Registrierung**.

3) Geben Sie Ihre Daten ein und klicken Sie auf **Abschicken**.

4) Klicken Sie im Navigationsbaum auf **Lizenz Online aktivieren**.

5) Geben Sie im Feld **Lizenz Autorisierungs Code (LAC)** den LAC ein.

6) Aktivieren Sie das Kontrollkästchen **Ich habe Benutzernamen und Kennwort für den Lizenzserver und möchte mich anmelden**.

7) Geben Sie **Benutzername** und **Kennwort** für die Anmeldung am Lizenzserver ein.

8) Klicken Sie auf **Aktivieren**. Die Verbindung zum Lizenzserver wird hergestellt und die Lizenzen in das Kommunikationssystem übertragen. Nach erfolgreicher Freischaltung wird die Verbindung automatisch wieder abgebaut.

7.3.1.2 Wie Sie Lizenzen offline aktivieren (Standalone)

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.
- Die Lizenzdatei wurde am zentralen Lizenzserver erzeugt und abgespeichert. Sie kennen den Ablageort der Lizenzdatei.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.

2) Klicken Sie im Navigationsbaum auf **Lizenzdatei aktivieren**.

3) Klicken Sie unter **Lizenzdatei** auf **Durchsuchen** und wählen Sie den Ablageort der Lizenzdatei aus.

4) Klicken Sie auf **Aktivieren**.

7.3.2 Lizenzzuordnung (Standalone)

Nach erfolgreicher Lizenzaktivierung müssen die erworbenen Lizenzen den Teilnehmern und den Leitungen zugeordnet werden. Systemweite Leistungsmerkmale sind in einem Standalone-System bereits mit der Aktivierung freigeschaltet.

Zuordnung von Teilnehmer-Lizenzen und User-orientierten Lizenzen

Den Teilnehmern können Teilnehmer-Lizenzen und User-orientierte Lizenzen zugeordnet werden.

Folgenden Teilnehmer-Typen können Teilnehmer-Lizenzen zugeordnet werden:

Icon	Teilnehmer-Lizenz	Beschreibung
	IP-Teilnehmer	für die Nutzung von IP-Systemtelefonen (HFA oder SIP) und SIP-Telefonen
	TDM-Teilnehmer	für die Nutzung von UP0-Systemtelefonen, ISDN-Telefonen, analogen Telefonen und DECT-Telefonen
	Mobiler Teilnehmer	für die Nutzung von myPortal for Mobile/Tablet, myPortal to go, Mobility Entry und DISA (One Number Service)
	DeskSharing-Teilnehmer	für die Nutzung von DeskSharing für IP-Teilnehmer

Die Teilnehmer-Lizenzen werden den Rufnummern der Teilnehmer fest zugeordnet. Wird ein Teilnehmer gelöscht oder einer Rufnummer ein anderer Teilnehmer-Typ zugeordnet, wird die zugehörige Teilnehmer-Lizenz freigegeben.

Mit der flexiblen Teilnehmer-Lizenzierung können TDM-, Mobility- und DeskShare User auch mit IP User Lizenzen lizenziert werden. Sind alle erworbenen TDM-, DeskShare- und Mobility User Lizenzen den Teilnehmern zugeordnet und besteht Bedarf für weitere TDM-, DeskShare- und Mobility User, können übrige IP User Lizenzen verwendet werden, um diesen Bedarf zu decken.

Nachdem dem Teilnehmer eine Teilnehmer-Lizenz zugewiesen wurde, können dem Teilnehmer auch User-orientierte Lizenzen zugewiesen werden.

Folgende User-orientierte Lizenzen können den Teilnehmern zugeordnet werden:

Icon	User-orientierte Lizenz	Beschreibung
	Voicemail	für die Nutzung der Sprachbox.
	UC Smart	für die Nutzung der UC Smart Funktionen über myPortal Smart.
	Groupware User	für die Nutzung der UC Suite Funktionen über myPortal for Outlook.
	UC Suite	für die Nutzung der UC Suite Funktionen über myPortal for Desktop.
	Fax	für die Nutzung einer Faxbox innerhalb der UC Suite. Voraussetzung eine UC User oder eine Groupware User Lizenz.
	Conference	für die Nutzung der Konferenz-Funktionen der UC Suite. Voraussetzung ist eine UC User oder eine Groupware User Lizenz.
	myAttendant	für die Nutzung der UC Suite Vermittlungsfunktionen.
	myAgent	für die Nutzung der Contact Center Funktionen.
	Application Launcher	für die anrufbezogene Steuerung von Applikationen auf einem Client-PC bei ankommenden und gehenden Anrufen, z. B. Aufruf einer Applikation oder Anzeige von Anruferdaten.
	TAPI 120/170	für die Nutzung von TAPI-konformen Applikationen und PC-unterstütztes Telefonieren mit kundeneigenen Programmen verschiedener Software-Hersteller.

Sie können sich eine Übersicht über alle Teilnehmer-Lizenzen und User-orientierte Lizenzen anzeigen lassen (**über Lokale Benutzerlizenzen > Überblick)**.

In dieser Übersicht werden Ihnen auch zu jedem Teilnehmer die Zustände seiner Lizenzen angezeigt.

Es gibt folgende Lizenzzustände:

Symbol	Erklärung
	Erfolgreich lizenziert.
	Lizenzfreigabe nicht gespeichert.
	Nicht lizenziert.
	Lizenzbedarf-Freigabe nicht gespeichert.
	Lizenzbedarf konfigurierbar.
	Lizenzbedarf nicht gespeichert.
	Lizenzbedarf nicht konfigurierbar.

Zuordnung von Systemlizenzen

Systemlizenzen enthalten Lizenzen für Leitungen und für systemweite Leistungsmerkmale.

Folgenden Leitungen können Lizenzen zugeordnet werden:

- S_{2M}-/T1-Leitungen: Anzahl der B-Kanäle
- ITSP-Leitungen: Anzahl der gleichzeitig über einen ITSP geführten Gespräche

Lizenzen für systemweite Leistungsmerkmale werden bei einem Standalone-System bereits bei der Lizenzaktivierung standardmäßig freigeschaltet. Eine weitere Zuordnung ist nicht nötig.

Vorgehensweise bei der Lizenzzuordnung

Voraussetzung: Die Lizenzdatei ist aktiviert und die Teilnehmer sind eingerichtet.

- Teilnehmer lizenzieren

  a) Teilnehmer eine Teilnehmer-Lizenz zuordnen. Durch diese Zuordnung wird für den Teilnehmer eine Lizenzanforderung generiert und zugleich die Zuweisung der User-orientierten Lizenzen freigeschaltet.

  b) Teilnehmer die User-orientierten Lizenzen zuordnen. Durch diese Zuordnungen werden für den Teilnehmer weitere Lizenzanforderungen generiert. Bitte beachten Sie, dass einige Lizenzen andere Lizenzen voraussetzen (siehe *Vorschläge für Lizenzkombinationen*).

  c) Lizenzanforderungen prüfen und freischalten.

  d) Liegen nicht genügend Lizenzen für die Freischaltung vor, werden Ihnen die fehlerhaften Zuordnungen über die Lizenzzustände (rot) angezeigt. Die Lizenzzuordnungen korrigieren und die Lizenzen erneut prüfen und freischalten.

INFO: Zur besseren Übersicht können Sie sich die Lizenzzuordnungen für alle Teilnehmer als Vorab-Ausdruck anzeigen lassen (**über Lokale Benutzerlizenzen > Überblick > Drucken**). Am Ende des Ausdrucks werden alle fehlerhaften Zuordnungen in einer separaten Tabelle aufgeführt.

- Leitungen lizenzieren
  Die Leitungslizenzen müssen auf die benötigten S_{2M}-/T1-Leitungen und auf die benötigten ITSP-Leitungen aufgeteilt werden.

Verwandte Themen

- Lizenzierung eines Kommunikationssystems (Standalone)
- Lizenzaktivierung (Standalone)
- Teilnehmer-Lizenzen

7.3.2.1 Wie Sie Teilnehmer lizenzieren (Standalone)

Verteilen Sie die verfügbaren Teilnehmer-Lizenzen und User-orientierten Lizenzen auf die Teilnehmer. Nach erfolgreicher Zuordnung sind die Teilnehmer lizenziert.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

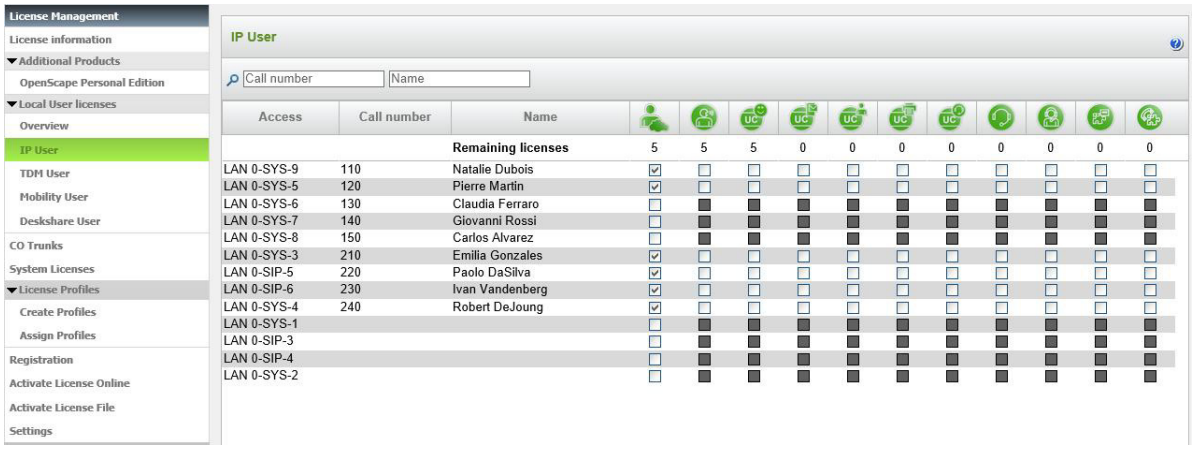
1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.

2) Navigieren Sie im Navigationsbaum auf **Lokale Benutzerlizenzen > ...** zum gewünschten Teilnehmer-Typ. Es wird Ihnen eine Liste aller Teilnehmer des ausgewählten Teilnehmer-Typs angezeigt.

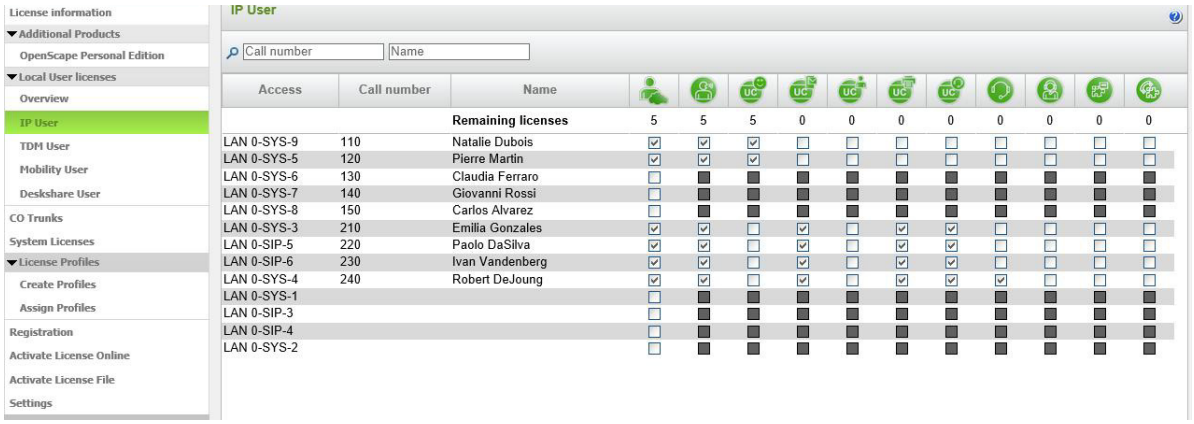
Unter **verbleibende Lizenzen** wird Ihnen angezeigt, wie viele Lizenzen Sie noch den Teilnehmern zuordnen können. Bei den TDM-, Mobility- und DeskShare-Teilnehmern beinhaltet die Anzeige auch alle noch übrigen IP User Lizenzen, da diese Lizenzen auch für die Lizenzierung von TDM-, Mobility- und DeskShare-Teilnehmern verwendet werden dürfen (flexible Teilnehmer-Lizenzierung).

3) Aktivieren Sie in der Zeile des gewünschten Teilnehmers die Teilnehmer-Lizenz, indem Sie das hell hinterlegte Kontrollkästchen (erste Spalte mit Kontrollkästchen) aktivieren. Die Kontrollkästchen in den anderen Spalten werden freigeschaltet.

INFO: Sie können sich auch einen ausgewählten Teilnehmer anzeigen lassen, indem Sie in die Suchfelder **Rufnummer** oder **Name** den Suchbegriff eingeben und anschließend die Return-Taste drücken oder auf das Lupen-Symbol klicken. Alle Teilnehmer werden aufgelistet, wenn beide Suchfelder leer sind und Sie anschließend die Return-Taste drücken oder auf das Lupen-Symbol klicken.



4) Aktivieren Sie in der Zeile des gewünschten Teilnehmers die User-orientierten Lizenzen, indem Sie die gewünschten Kontrollkästchen aktivieren.



> ***INFO:*** User-orientierte Lizenzen können einem Teilnehmer nur zugewiesen werden, wenn dem Teilnehmer zuvor eine Teilnehmer-Lizenz zugeordnet wurde (Schritt 3).

5) Klicken Sie auf **OK & Weiter**. Es wird geprüft, ob für Ihre Zuordnung genügend Lizenzen vorhanden sind.

Sind ausreichend Lizenzen vorhanden, ist die Lizenzierung der Teilnehmer hiermit beendet.

6) Fehlen Lizenzen, werden Ihnen die Fehler mit rot hinterlegten Kontrollkästchen angezeigt. Korrigieren Sie diese Fehler und wiederholen Sie Schritt 5.

> ***INFO:*** Wenn Sie eine Teilnehmer-Lizenz entfernen wollen, müssen Sie eine Warnmeldung bestätigen. Anschließend erscheint ein neues Kontrollkästchen **Warnungen aktiviert**. Wenn Sie dieses Kontrollkästchen deaktivieren, können Sie weitere Teilnehmer-Lizenzen ohne Warnmeldung entfernen.

7.3.2.2 Wie Sie Leitungen lizenzieren (Standalone)

Verteilen Sie die erworbenen Leitungslizenzen auf die SIP- und S_{2M}-/T1-Leitungen.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.

2) Klicken Sie im Navigationsbaum auf **Amtsleitungen**. Im Bereich **Amtsleitungen** wird Ihnen die Anzahl der verfügbaren Lizenzen für SIP- und S_{2M}-/T1-Amtsleitungen angezeigt.

3) Für SIP-Leitungen: Geben Sie im Bereich **SIP trunks** unter **Bedarf an Lizenzen für gleichzeitige Internet-Anrufe in diesem Knoten** die Anzahl der Internet-Gespräche an, die gleichzeitig über einen ITSP geführt werden können.

4) Für S_{2M}-Leitungen: Wählen Sie im Bereich **PRI (S2M/T1)** in der Zeile des gewünschten S_{2M}-Slots in der Aufklappliste der Spalte **Demands** die Anzahl der gewünschten B-Kanäle aus.

5) Für digitale T1-Leitungen (nur USA): Wählen Sie im Bereich **PRI (S2M/T1)** in der Zeile des gewünschten T1-Slots in der Aufklappliste der Spalte **Demands** die Anzahl der gewünschten B-Kanäle aus.

6) Für analoge T1-Leitungen (nur USA): Aktivieren Sie die analoge T1-Leitung, indem Sie im Bereich **PRI (S2M/T1)** in der Zeile der analoge T1-Leitung in der Aufklappliste der Spalte **Demands** den Eintrag **1** auswählen (**0** bedeutet: die Leitung ist deaktiviert).

7) Klicken Sie auf **OK & Weiter**.

INFO: Die Anzahl der lizenzierten SIP-Leitungen und die Anzahl der lizenzierten S_{2M}-/T1-Leitungen darf die Anzahl der verfügbaren Leitungslizenzen nicht überschreiten.

7.4 Lizenzierung mehrerer Kommunikationssysteme (Netzverbund)

Die Lizenzierung mehrerer Kommunikationssysteme ist in einer bestimmten Reihenfolge durchzuführen. Diese Reihenfolge ist am Beispiel eines Netzverbunds aus einer OpenScape Business S (Master) und zweier OpenScape Business X3 (Slave) dargestellt.

Sind mehrere OpenScape Business (Knoten) zu einem Netzverbund zusammengeschlossen, erfolgt die Lizenzierung zentral über eine Netzwerklizenzdatei, die am Master-Knoten aktiviert wird. Zusätzlich benötigt jeder Slave-Knoten im Netzverbund eine eigene Networking-Systemlizenz. Der Knoten mit der größten Bandbreite sollte der Master-Knoten sein.

Mit dem Netzwerk-Wizard des WBM werden die Knoten im Netzverbund als Master-Knoten und Slave-Knoten konfiguriert. Der Master-Knoten enthält den zentralen Lizenzagenten (zentraler CLA, central Customer License Agent). Alle Slave-Knoten im Netzverbund nutzen diesen CLA für die Lizenzierung. Dafür wird den Slave-Knoten mit Hilfe des WBM die IP-Adresse des Master-Knotens bekannt gegeben.

Für den gesamten Netzverbund existiert nur eine Netzwerklizenzdatei. Diese ist an den Master-Knoten über seine Locking ID gebunden. Ist eine OpenScape Business S (Soft Switch) der Master-Knoten, ist die Netzwerklizenzdatei über die Locking ID des Linux-Servers des Soft Switches oder über die Advanced Locking ID des Soft Switches gebunden, wenn der Soft Switch in einer virtuellen Umgebung eingesetzt wird. Die Netzwerklizenzdatei ist im zentralen CLA gespeichert und enthält alle Lizenzinformationen des Netzverbunds. Sie kann nur am Master-Knoten über das WBM aktiviert werden. Nur der Master-Knoten hat Zugang zum CLS, an allen anderen Knoten ist der Zugang deaktiviert.

Im Netzverbund sollte eine knotenspezifische Lizenzierung nicht vorgenommen werden. Liegt für jeden Knoten bereits eine eigene Netzwerkdatei vor, können Sie diese am CLS zu einer Netzwerklizenzdatei zusammenführen.

Verhalten bei Netzproblemen (Failover)

Fällt die Verbindung zum Master-Knoten und somit zum zentralen CLA aus, wird im Display der Systemtelefone "Failover Period" angezeigt. Innerhalb dieser Failover Period (max. 30 Tage) sind alle Knoten und deren Leistungsmerkmale weiterhin funktionsfähig. Sind die Netzprobleme beseitigt und ist die Verbindung zum zentralen CLA wiederhergestellt, gehen alle Knoten wieder in den regulären Lizenzstatus über.

Werden die Netzprobleme nicht innerhalb der Failover Period behoben, gehen die Knoten in den Notbetrieb über. Anschließend muss der Netzverbund neu lizenziert werden.

Lizenzierungsablauf im Netzverbund anhand des o.g. Beispiels

OpenScape Business S (Master) und beide OpenScape Business X3 (Slave) sind bereits installiert, konfiguriert und zu einem Netzverbund zusammengeschlossen.

1. **Lizenz-Autorisierungscode (LAC)**
   Der Kunde erhält beim Kauf von Lizenzen einen Lizenz-Autorisierungscode (LAC). Die Daten über die erworbenen Lizenzen sind in der Datenbank des zentralen Lizenzservers (CLS) gespeichert.

2. **OpenScape Business S als Master-Knoten**
   Der Kunde oder Servicetechniker meldet sich am WBM der OpenScape Business S an und installiert mit Hilfe des Netzwerk-Wizards die OpenScape Business S als Master-Knoten.
   Beschreibung siehe *Szenario 3: Konfiguration*
   Das System wurde bereits installiert und konfiguriert und läuft in der Activation Period (Zeitspanne von 30 Tagen, in der die Lizenzierung vorgenommen werden muss).
3. **Locking ID des Master-Knotens**
   Der Kunde oder Servicetechniker notiert sich die Locking ID oder die Advanced Locking ID von OpenScape Business S.
   Beschreibung siehe *Wie Sie die Locking ID des Kommunikationssystems abfragen*
4. **OpenScape Business X3 als Slave-Knoten**
   Der Kunde oder Servicetechniker meldet sich zuerst am WBM der ersten OpenScape Business X3 an und installiert mit Hilfe des Netzwerk-Wizards die erste OpenScape Business X3 als Slave-Knoten und wiederholt diese Prozedur am WBM der zweiten OpenScape Business X3.
   Beschreibung siehe *Szenario 3: Konfiguration*
   Die Systeme wurden bereits installiert und konfiguriert und laufen in der Activation Period.
5. **Locking IDs von OpenScape Business X3**
   Der Kunde oder Servicetechniker notiert sich die Locking IDs der beiden OpenScape Business X3.
   Beschreibung siehe *Wie Sie die Locking ID des Kommunikationssystems abfragen*
6. **Lizenzaktivierung**
   Der Kunde oder Servicetechniker meldet sich am CLS an und generiert zusammen mit dem Lizenz-Autorisierungscode und den Locking IDs eine Netzwerklizenzdatei. Diese Datei lädt er mit Hilfe des WBM in den Master-Knoten.
   Beschreibung siehe *Wie Sie Lizenzen offline aktivieren (Netzverbund)*
   Das System aktiviert daraufhin die erworbenen Lizenzen.
7. **Lizenzzuordnung**
   Der Kunde oder Servicetechniker verteilt nun die Lizenzen auf die Knoten. Dazu meldet er sich am WBM jedes Knotens an und ordnet dem Knoten die gewünschte Anzahl von Lizenzen zu. Wichtig ist, dass jedem Knoten eine Networking-Systemlizenz zugewiesen ist, ansonsten ist er nicht in den Netzverbund integriert.
   Beschreibung siehe *Wie Sie Systemlizenzen einem Knoten zuordnen*

7.4.1 Lizenzaktivierung (Netzverbund)

Nachdem ein Produkt oder ein Leistungsmerkmal erworben wurde, müssen zuerst die mit dem Produkt/Leistungsmerkmal bereitgestellten Lizenzen aktiviert werden. Dafür wird direkt die Lizenzdatei benötigt. Nach erfolgreicher Aktivierung erfolgt dann die Lizenzzuordnung.

Um Lizenzen zu aktivieren gibt es folgende Möglichkeit:

- **Offline-Lizenzaktivierung** (direkt über die Lizenzdatei)
  Der Kunde oder Servicetechniker meldet sich am zentralen Lizenzserver (CLS) an und gibt dort den Lizenz-Autorisierungscode zusammen mit den Locking IDs der Kommunikationssysteme ein. Der CLS erzeugt aus den Daten eine Lizenzdatei. Der Kunde oder Servicetechniker lädt sich die Lizenzdatei herunter und spielt diese in das WBM des Master-Knotens ein.
  Am Master-Knoten wird geprüft, ob die in der Lizenzdatei gespeicherten Locking IDs mit denen der Systeme übereinstimmen. Ist die Prüfung erfolgreich, werden die Lizenzen aktiviert und die Systeme wechseln in den regulären Lizenzstatus. Ist die Prüfung nicht erfolgreich, laufen die Systeme weiter in der Activation Period und nach Ablauf der Activation Period nur noch im Notbetrieb.
  Die IP-Adresse des CLS ist im WBM unter **Lizenzverwaltung > Einstellungen** hinterlegt.

Um Lizenzdateien zusammen zu führen gibt es folgende Möglichkeit:

- **Lizenzdateien zu einer Netzwerklizenzdatei zusammenführen**
  Sind bereits ein oder mehrere Knoten lizenziert und sollen diese in einem Netzverbund zusammengeführt werden, so muss der Administrator über den CLS die einzelnen Lizenzdateien zu einer Netzwerklizenzdatei zusammenführen und diese in den zentralen CLA laden. An allen anderen Knoten muss die IP-Adresse des Master-Knotens mit dem zentralen Lizenzagenten über den Netzwerk-Wizard des WBM eingegeben werden.

7.4.1.1 Wie Sie Lizenzen offline aktivieren (Netzverbund)

Am Beispiel einer OpenScape Business S als Master-Knoten (Knoten 1) und zwei weiteren OpenScape Business X3 (Knoten 2 und Knoten 3) wird die Generierung und Aktivierung der gemeinsamen Netzwerklizenzdatei beschrieben.

Voraussetzungen

- Es besteht ein Zugang zum CLS.
- Alle Knoten sind installiert und miteinander vernetzt, siehe *Szenario 3: Vernetzung von Open Scape Business X und OpenScape Business S (Multi Gateway)*.

Schritt für Schritt

1) Melden Sie sich am CLS mit Ihrem Benutzernamen und Passwort an.

2) Wählen Sie unter **Lizenzen** den Eintrag **Lizenzschlüssel generieren und herunterladen**.

3) Geben Sie unter **LAC** den Lizenz-Autorisierungscode (LAC) ein und klicken Sie auf **Suchen**.

4) Öffnen Sie das Produkt OpenScape Business S und wählen Sie die Leistungsmerkmale aus, die dem Knoten 1 zugeordnet werden sollen.

5) Klicken Sie auf **Lizenzschlüssel generieren**.

6) Geben Sie unter **MAC Adresse** die MAC-Adresse oder Advanced Locking ID von OpenScape Business S (Knoten 1) ein und unter **MAC-Adresse des Netzwerk-CLA** nochmal die MAC-Adresse oder Advanced Locking ID von OpenScape Business S (Master-Knoten) ein.

INFO: Die MAC-Adresse von OpenScape Business S ist die MAC-Adresse der Netzwerkkarte des OpenScape Business S Linux-Servers, die bei der Installation des Linux-Betriebssystems verwendet wurde. Die Advanced Locking ID von OpenScape Business S wird anstelle der MAC-Adresse verwendet, wenn OpenScape Business S in einer virtuellen Umgebung betrieben wird.

---

7) Geben Sie bei den Leistungsmerkmalen die gewünschte Anzahl ein und klicken Sie auf **Weiter**.

8) Kontrollieren Sie die Kundendaten und klicken Sie auf **Weiter**.

9) Lesen Sie sich den rechtlichen Hinweis durch und klicken Sie anschließend auf **Ich stimme diesen Bedingungen zu**.

10) Klicken Sie auf **Ausführen**, um den Lizenzschlüssel generieren zu lassen.

11) Wählen Sie für den Knoten 2 unter **Lizenzen** den Eintrag **Lizenzschlüssel generieren und herunterladen**.

12) Geben Sie unter **LAC** erneut den Lizenz-Autorisierungscode (LAC) ein und klicken Sie auf **Suchen**.

13) Öffnen Sie das Produkt OpenScape Business X3 und wählen Sie die Leistungsmerkmale aus, die dem Knoten 2 zugeordnet werden sollen.

14) Klicken Sie auf **Lizenzschlüssel generieren**.

15) Geben Sie unter **MAC Adresse** die MAC-Adresse des Knoten 2 ein und unter **MAC-Adresse des Netzwerk-CLA** die MAC-Adresse des Knoten 1 (Master-Knoten) ein.

16) Geben Sie bei den Leistungsmerkmalen die gewünschte Anzahl ein und klicken Sie auf **Weiter**.

17) Klicken Sie auf **Weiter**.

18) Bestätigen Sie den rechtlichen Hinweis, indem Sie das Kontrollkästchen **Ich stimme diesen Bedingungen zu** anklicken.

19) Klicken Sie auf **Ausführen**, um den Lizenzschlüssel generieren zu lassen.

20) Wiederholen Sie die Schritte 11 bis 19 für den Knoten 3.

21) Klicken Sie auf **Lizenzschlüssel** und anschließend auf **Download**, um die Netzwerklizenzdatei herunterzuladen.

22) Speichern Sie die Netzwerklizenzdatei.

23) Melden Sie sich am WBM des Master-Knotens an, indem Sie in Ihrem Webbrowser die Adresse `https://<IP-Adresse des Master-Knotens>` aufrufen und anschließend Benutzernamen und Passwort eingeben.

24) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.

25) Klicken Sie im Navigationsbaum auf **Lizenzdatei aktivieren**.

26) Klicken Sie unter **Lizenzdatei** auf **Durchsuchen** und wählen Sie den Ablageort der Netzwerklizenzdatei aus.

27) Klicken Sie auf **Aktivieren**.

7.4.1.2 Wie Sie Lizenzdateien zu einer Netzwerklizenzdatei zusammenführen

Werden mehrere vorher nicht vernetzte Knoten in einen Netzverbund integriert, müssen die Lizenzdateien der einzelnen Knoten mit Hilfe des CLS zu einer gemeinsamen Netzwerklizenzdatei zusammengeführt werden.

Voraussetzungen

- Es besteht ein Zugang zum CLS und Sie besitzen die Zugriffsrechte für die Lizenzpakete der einzelnen Knoten.
- Alle Knoten sind installiert und miteinander vernetzt, siehe *Szenario 3: Vernetzung von Open Scape Business X und OpenScape Business S (Multi Gateway)*.

Schritt für Schritt

1) Melden Sie sich am CLS mit Ihrem Benutzernamen und Passwort an.

2) Wählen Sie unter **Netzwerk Lizenzierung** den Eintrag **System hinzufügen/ entfernen** aus.

3) Wählen Sie die MAC-Adresse des Knotens aus, der in den Netzverbund integriert werden soll.

4) Klicken Sie auf die **Rehost**.

5) Geben Sie unter **MAC-Adresse** die MAC-Adresse des Knotens ein.

6) Geben Sie unter **MAC-Adresse des Netzwerk-CLA** die MAC-Adresse des Master-Knotens ein. In der Regel ist OpenScape Business S der Master-Knoten.

> ***INFO:*** Die MAC-Adresse von OpenScape Business S ist MAC-Adresse der Netzwerkkarte des OpenScape Business S Linux-Servers, die bei der Installation des Linux-Betriebssystems verwendet wurde.

7) Klicken Sie auf **Weiter**.

8) Kontrollieren Sie die Kundendaten und klicken Sie auf **Weiter**.

9) Lesen Sie sich den rechtlichen Hinweis durch und klicken Sie anschließend auf **Ich stimme diesen Bedingungen zu**.

10) Klicken Sie auf **Ausführen**, um den Lizenzschlüssel generieren zu lassen.

11) Wiederholen Sie für weitere Knoten die Schritte 2 bis 10.

12) Klicken Sie auf **Lizenzschlüssel** und anschließend auf **Download**, um die Netzwerklizenzdatei herunterzuladen.

13) Speichern Sie die Netzwerklizenzdatei.

14) Melden Sie sich am WBM des Master-Knotens an, indem Sie in Ihrem Webbrowser die Adresse `https://<IP-Adresse des Master-Knotens>` aufrufen und anschließend Benutzernamen und Passwort eingeben.

15) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.

16) Klicken Sie im Navigationsbaum auf **Lizenzdatei aktivieren**.

17) Klicken Sie unter **Lizenzdatei** auf **Durchsuchen** und wählen Sie den Ablageort der Netzwerklizenzdatei aus.

18) Klicken Sie auf **Aktivieren**.

7.4.2 Lizenzzuordnung (Netzverbund)

Nach erfolgreicher Lizenzaktivierung müssen die erworbenen Lizenzen den Teilnehmern und den Leitungen zugeordnet werden. Diese Zuordnung wird an jedem Knoten separat durchgeführt.

Zuordnung von Teilnehmer-Lizenzen und User-orientierten Lizenzen

Den Teilnehmern können Teilnehmer-Lizenzen und User-orientierte Lizenzen zugeordnet werden.

Folgenden Teilnehmer-Typen können Teilnehmer-Lizenzen zugeordnet werden:

Icon	Teilnehmer-Lizenz	Beschreibung
	IP-Teilnehmer	für die Nutzung von IP-Systemtelefonen (HFA oder SIP) und SIP-Telefonen
	TDM-Teilnehmer	für die Nutzung von UP0-Systemtelefonen, ISDN-Telefonen, analogen Telefonen und DECT-Telefonen
	Mobiler Teilnehmer	für die Nutzung von myPortal for Mobile/Tablet, myPortal to go, Mobility Entry und DISA (One Number Service)
	DeskSharing-Teilnehmer	für die Nutzung von DeskSharing für IP-Teilnehmer

Die Teilnehmer-Lizenzen werden den Rufnummern der Teilnehmer fest zugeordnet. Wird ein Teilnehmer gelöscht oder einer Rufnummer ein anderer Teilnehmer-Typ zugeordnet, wird die zugehörige Teilnehmer-Lizenz freigegeben.

Mit der flexiblen Teilnehmer-Lizenzierung können TDM-, Mobility- und DeskShare User auch mit IP User Lizenzen lizenziert werden. Sind alle erworbenen TDM-, DeskShare- und Mobility User Lizenzen den Teilnehmern zugeordnet und besteht Bedarf für weitere TDM-, DeskShare- und Mobility User, können übrige IP User Lizenzen verwendet werden, um diesen Bedarf zu decken.

Nachdem dem Teilnehmer eine Teilnehmer-Lizenz zugewiesen wurde, können dem Teilnehmer auch User-orientierte Lizenzen zugewiesen werden.

Folgende User-orientierte Lizenzen können den Teilnehmern zugeordnet werden:

Icon	User-orientierte Lizenz	Beschreibung
	Voicemail	für die Nutzung der Sprachbox.
	UC Smart	für die Nutzung der UC Smart Funktionen über myPortal Smart.
	Groupware User	für die Nutzung der UC Suite Funktionen über myPortal for Outlook.
	UC Suite	für die Nutzung der UC Suite Funktionen über myPortal for Desktop.
	Fax	für die Nutzung einer Faxbox innerhalb der UC Suite. Voraussetzung eine UC User oder eine Groupware User Lizenz.
	Conference	für die Nutzung der Konferenz-Funktionen der UC Suite. Voraussetzung ist eine UC User oder eine Groupware User Lizenz.
	myAttendant	für die Nutzung der UC Suite Vermittlungsfunktionen.
	myAgent	für die Nutzung der Contact Center Funktionen.
	Application Launcher	für die anrufbezogene Steuerung von Applikationen auf einem Client-PC bei ankommenden und gehenden Anrufen, z. B. Aufruf einer Applikation oder Anzeige von Anruferdaten.
	TAPI 120/170	für die Nutzung von TAPI-konformen Applikationen und PC-unterstütztes Telefonieren mit kundeneigenen Programmen verschiedener Software-Hersteller.

Sie können sich eine Übersicht über alle Teilnehmer-Lizenzen und User-orientierte Lizenzen anzeigen lassen (**über Lokale Benutzerlizenzen > Überblick)**.

In dieser Übersicht werden Ihnen auch zu jedem Teilnehmer die Zustände seiner Lizenzen angezeigt.

Es gibt folgende Lizenzzustände:

Symbol	Erklärung
	Erfolgreich lizenziert.
	Lizenzfreigabe nicht gespeichert.
	Nicht lizenziert.
	Lizenzbedarf-Freigabe nicht gespeichert.
	Lizenzbedarf konfigurierbar.
	Lizenzbedarf nicht gespeichert.
	Lizenzbedarf nicht konfigurierbar.

Zuordnung von Systemlizenzen

Systemlizenzen enthalten Lizenzen für Leitungen und für systemweite Leistungsmerkmale.

Folgenden Leitungen können Lizenzen zugeordnet werden:

- S_{2M}-/T1-Leitungen: Anzahl der B-Kanäle
- ITSP-Leitungen: Anzahl der gleichzeitig über einen ITSP geführten Gespräche

Systemweite Lizenzen werden im Netzverbund jedem System (Knoten) zugeordnet. Diese Konfiguration ist direkt nacheinander an jedem Knoten durchzuführen. Die Gesamtzahl der systemweiten Lizenzen, die in der Netzwerklizenzdatei auf dem Master-Knoten gespeichert sind, wird um die an dem Knoten konfigurierte Anzahl reduziert.

Vorgehensweise bei der Lizenzzuordnung

Voraussetzung: Die Lizenzdatei ist aktiviert und die Teilnehmer sind eingerichtet.

- Teilnehmer lizenzieren
  a) Teilnehmer eine Teilnehmer-Lizenz zuordnen. Durch diese Zuordnung wird für den Teilnehmer eine Lizenzanforderung generiert und zugleich die Zuweisung der User-orientierten Lizenzen freigeschaltet.
  b) Teilnehmer die User-orientierten Lizenzen zuordnen. Durch diese Zuordnungen werden für den Teilnehmer weitere Lizenzanforderungen generiert. Bitte beachten Sie, dass einige Lizenzen andere Lizenzen voraussetzen (siehe *Vorschläge für Lizenzkombinationen*).
  c) Lizenzanforderungen prüfen und freischalten.
  d) Liegen nicht genügend Lizenzen für die Freischaltung vor, werden Ihnen die fehlerhaften Zuordnungen über die Lizenzzustände (rot) angezeigt. Die Lizenzzuordnungen korrigieren und die Lizenzen erneut prüfen und freischalten.

INFO: Zur besseren Übersicht können Sie sich die Lizenzzuordnungen für alle Teilnehmer als Vorab-Ausdruck anzeigen lassen (**über Lokale Benutzerlizenzen > Überblick > Drucken**). Am Ende des Ausdrucks werden alle fehlerhaften Zuordnungen in einer separaten Tabelle aufgeführt.

- Leitungen lizenzieren
  Die Leitungslizenzen müssen auf die benötigten S_{2M}-/T1-Leitungen und auf die benötigten ITSP-Leitungen aufgeteilt werden.

7.4.2.1 Wie Sie Teilnehmer lizenzieren (Netzverbund)

Verteilen Sie die verfügbaren Teilnehmer-Lizenzen und User-orientierten Lizenzen auf die Teilnehmer. Nach erfolgreicher Zuordnung sind die Teilnehmer lizenziert.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

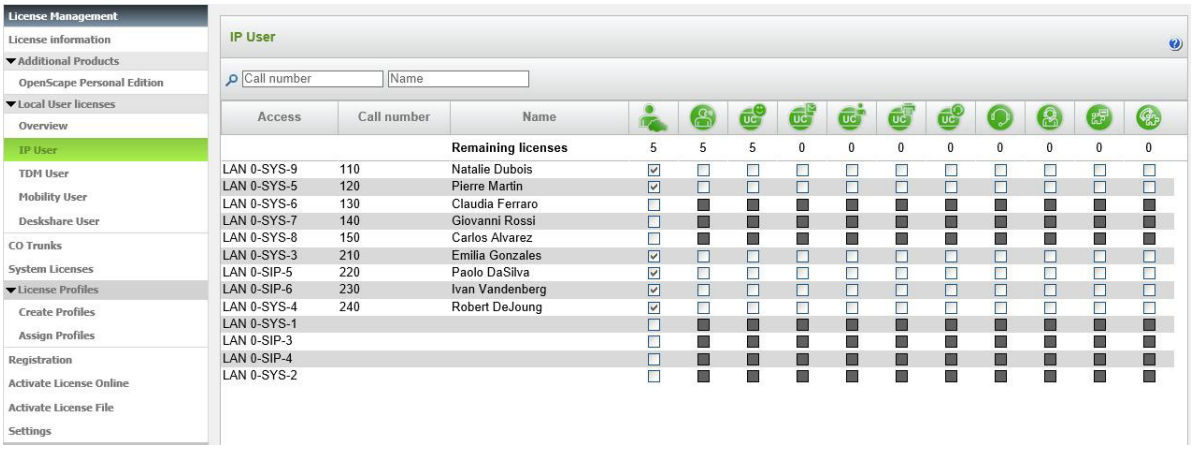
1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.

2) Navigieren Sie im Navigationsbaum auf **Lokale Benutzerlizenzen > ...** zum gewünschten Teilnehmer-Typ. Es wird Ihnen eine Liste aller Teilnehmer des ausgewählten Teilnehmer-Typs angezeigt.

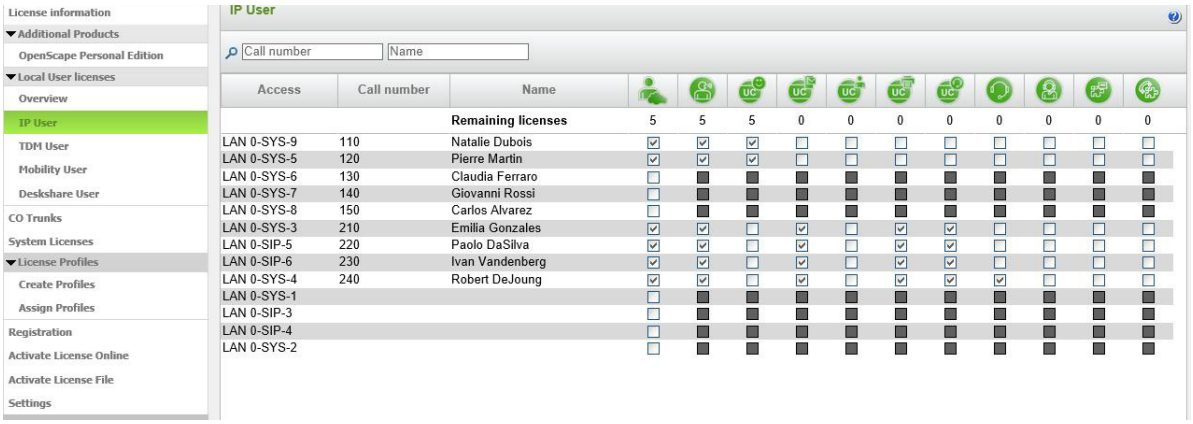
Unter **verbleibende Lizenzen** wird Ihnen angezeigt, wie viele Lizenzen Sie noch den Teilnehmern zuordnen können. Bei den TDM-, Mobility- und DeskShare-Teilnehmern beinhaltet die Anzeige auch alle noch übrigen IP User Lizenzen, da diese Lizenzen auch für die Lizenzierung von TDM-, Mobility- und DeskShare-Teilnehmern verwendet werden dürfen (flexible Teilnehmer-Lizenzierung).

3) Aktivieren Sie in der Zeile des gewünschten Teilnehmers die Teilnehmer-Lizenz, indem Sie das hell hinterlegte Kontrollkästchen (erste Spalte mit Kontrollkästchen) aktivieren. Die Kontrollkästchen in den anderen Spalten werden freigeschaltet.

INFO: Sie können sich auch einen ausgewählten Teilnehmer anzeigen lassen, indem Sie in die Suchfelder **Rufnummer** oder **Name** den Suchbegriff eingeben und anschließend die Return-Taste drücken oder auf das Lupen-Symbol klicken. Alle Teilnehmer werden aufgelistet, wenn beide Suchfelder leer sind und Sie anschließend die Return-Taste drücken oder auf das Lupen-Symbol klicken.



4) Aktivieren Sie in der Zeile des gewünschten Teilnehmers die User-orientierten Lizenzen, indem Sie die gewünschten Kontrollkästchen aktivieren.



INFO: User-orientierte Lizenzen können einem Teilnehmer nur zugewiesen werden, wenn dem Teilnehmer zuvor eine Teilnehmer-Lizenz zugeordnet wurde (Schritt 3).

5) Klicken Sie auf **OK & Weiter**. Es wird geprüft, ob für Ihre Zuordnung genügend Lizenzen vorhanden sind.

Sind ausreichend Lizenzen vorhanden, ist die Lizenzierung der Teilnehmer hiermit beendet.

6) Fehlen Lizenzen, werden Ihnen die Fehler mit rot hinterlegten Kontrollkästchen angezeigt. Korrigieren Sie diese Fehler und wiederholen Sie Schritt 5.

INFO: Wenn Sie eine Teilnehmer-Lizenz entfernen wollen, müssen Sie eine Warnmeldung bestätigen. Anschließend erscheint ein neues Kontrollkästchen **Warnungen aktiviert**. Wenn Sie dieses Kontrollkästchen deaktivieren, können Sie weitere Teilnehmer-Lizenzen ohne Warnmeldung entfernen.

7.4.2.2 Wie Sie Leitungen lizenzieren (Netzverbund)

Verteilen Sie die erworbenen Leitungslizenzen auf die SIP- und S_{2M}-/T1-Leitungen.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.

2) Klicken Sie im Navigationsbaum auf **Amtsleitungen**. Im Bereich **Amtsleitungen** wird Ihnen die Anzahl der verfügbaren Lizenzen für SIP- und S_{2M}-/T1-Amtsleitungen angezeigt.

3) Für SIP-Leitungen: Geben Sie im Bereich **SIP trunks** unter **Bedarf an Lizenzen für gleichzeitige Internet-Anrufe in diesem Knoten** die Anzahl der Internet-Gespräche an, die gleichzeitig über einen ITSP geführt werden können.

4) Für S_{2M}-Leitungen: Wählen Sie im Bereich **PRI(S2M/T1)** in der Zeile des gewünschten S_{2M}-Slots in der Aufklappliste der Spalte **Demands** die Anzahl der gewünschten B-Kanäle aus.

5) Für T1-Leitungen (nur USA): Wählen Sie im Bereich **PRI(S2M/T1)** in der Zeile des gewünschten T1-Slots in der Aufklappliste der Spalte **Demands** die Anzahl der gewünschten B-Kanäle aus.

6) Klicken Sie auf **OK & Weiter**.

INFO: Die Anzahl der lizenzierten SIP-Leitungen und die Anzahl der lizenzierten S_{2M}-/T1-Leitungen darf die Anzahl der verfügbaren Leitungslizenzen nicht überschreiten.

7.4.2.3 Wie Sie Systemlizenzen einem Knoten zuordnen

Voraussetzungen

- Sie sind am WBM des gewünschten Knotens angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.

2) Klicken Sie im Navigationsbaum auf **System-Lizenzen**. Es werden Ihnen alle verfügbaren Systemlizenzen angezeigt.

3) Wählen Sie in der Spalte **benutzte Lizenzen** bei den gewünschten Systemlizenzen die Anzahl der Systemlizenzen aus, die dem Knoten zugeordnet werden sollen.

In der Spalte **verfügbar für Verteilung** wird Ihnen angezeigt, wie viele Lizenzen für den gesamten Netzverbund zur Verfügung stehen.

INFO: Achten Sie darauf, dass dem Knoten die Systemlizenz "Networking" zugeordnet ist, ansonsten ist der Konten nicht in den Netzverbund integriert.

---

4) Klicken Sie auf **Sichern**.

7.4.2.4 Wie Sie die Systemlizenz "Networking" einem Knoten zuordnen

Voraussetzungen

- Sie sind am WBM des gewünschten Knotens angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.

2) Klicken Sie im Navigationsbaum auf **System-Lizenzen**. Es werden Ihnen alle verfügbaren Systemlizenzen angezeigt.

3) Wählen Sie bei der Systemlizenz **Networking** in der Spalte **benutzte Lizenzen** aus der Aufklappliste den Eintrag **1** aus.

In der Spalte **verfügbar für Verteilung** wird Ihnen angezeigt, wie viele Lizenzen für den gesamten Netzverbund zur Verfügung stehen.

4) Klicken Sie auf **Sichern**.

7.5 Lizenzinformationen

Informationen zu den zur Verfügung stehenden und zugewiesenen Lizenzen, Produkten und Leistungsmerkmalen werden mit dem WBM angezeigt. Im Netzverbund können die Lizenzinformationen zu allen im Netz vorhandenen Knoten abgerufen werden.

Folgende Informationen können angezeigt werden:

- **MAC-Adresse**: MAC-Adresse der Hardware-Plattform oder des Softswitch Linux Servers, an die die Lizenzen gebunden sind.

INFO: Befindet sich das Kommunikationssystem in der Activation Period, wird hier evtl. eine falsche MAC-Adresse angezeigt. Die richtige MAC-Adresse kann über das Service-Center unter Inventory abgefragt werden (*Inventory*).

- **Advanced Locking ID**: Advanced Locking ID des Softswitches in einer virtuellen Umgebung, an die die Lizenzen gebunden sind.
- **Locking ID**: Locking ID des Application Servers, an die die Lizenzen gebunden sind.
- **Knoten**: Name des Kommunikationssystems, an die die Lizenzen gebunden sind.
- **Produktname**: Name des Produkts, das der Lizenz zugeordnet ist.
- **Leistungsmerkmal**: Leistungsmerkmal, das der Lizenz zugeordnet ist.
- **benutzte Lizenzen**: Anzeige der benutzten und der vorhandenen Lizenzen.
- **verteilbare Lizenzen**: Anzeige der im Netzverbund noch verfügbaren Lizenzen.
- **Status**: Status der Lizenz.

Das Produkt OpenScape Personal Edition ist über eine eigene Lizenzdatei lizenziert. Die Lizenzinformationen dazu werden unter **Zusätzliche Produkte** angezeigt.

7.5.1 Lizenzinformationen ohne Netzverbund (Standalone)

Es können alle dem Kommunikationssystem zugeordneten Lizenzen und die Informationen dazu angezeigt werden.

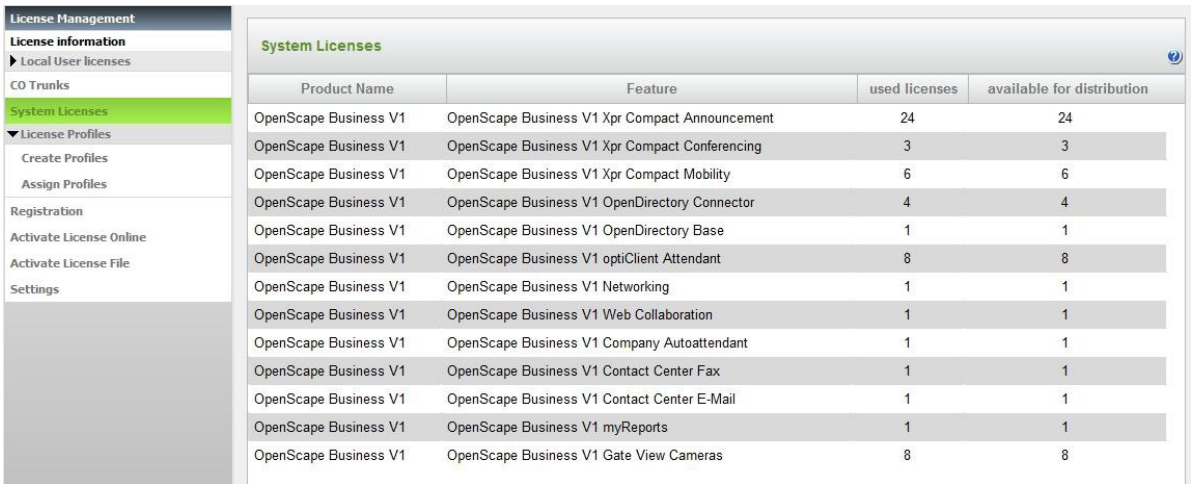
7.5.1.1 Wie Sie Lizenzinformationen anzeigen

Voraussetzungen

- Sie sind am WBM angemeldet.

Schritt für Schritt

› Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**. Es werden Ihnen die Lizenzinformationen zu Ihrem Kommunikationssystem angezeigt.



Product Name	Feature	used licenses	available for distribution
OpenScape Business V1	OpenScape Business V1 Xpr Compact Announcement	24	24
OpenScape Business V1	OpenScape Business V1 Xpr Compact Conferencing	3	3
OpenScape Business V1	OpenScape Business V1 Xpr Compact Mobility	6	6
OpenScape Business V1	OpenScape Business V1 OpenDirectory Connector	4	4
OpenScape Business V1	OpenScape Business V1 OpenDirectory Base	1	1
OpenScape Business V1	OpenScape Business V1 optiClient Attendant	8	8
OpenScape Business V1	OpenScape Business V1 Networking	1	1
OpenScape Business V1	OpenScape Business V1 Web Collaboration	1	1
OpenScape Business V1	OpenScape Business V1 Company Autoattendant	1	1
OpenScape Business V1	OpenScape Business V1 Contact Center Fax	1	1
OpenScape Business V1	OpenScape Business V1 Contact Center E-Mail	1	1
OpenScape Business V1	OpenScape Business V1 myReports	1	1
OpenScape Business V1	OpenScape Business V1 Gate View Cameras	8	8

7.5.2 Lizenzinformationen im Netzverbund

In einem Netzverbund können alle Lizenzen und die Informationen dazu angezeigt werden. Diese Informationen werden aus der Netzwerklizenzdatei ausgelesen.

Die Lizenzen in einem Netzverbund sind bis auf die Basis-Lizenzen vom Typ "floating" und befinden sich in einem Lizenz-Pool. Wird eine Lizenz an einem Knoten (Kommunikationssystem) nicht mehr benötigt und freigegeben, kann sie an einem anderen Knoten genutzt werden.

In einem Netzverbund können sowohl alle Lizenzen des Netzverbundes als auch die gemeinsam genutzten Lizenzen (floating) oder die speziell an einen Knoten gebundenen Lizenzen angezeigt werden.

Zusätzlich können die Teilnehmer-Lizenzen und die User-orientierten Lizenzen nach Knoten sortiert in einer Übersicht angezeigt werden.

7.5.2.1 Wie Sie alle Lizenzen des Netzverbundes anzeigen

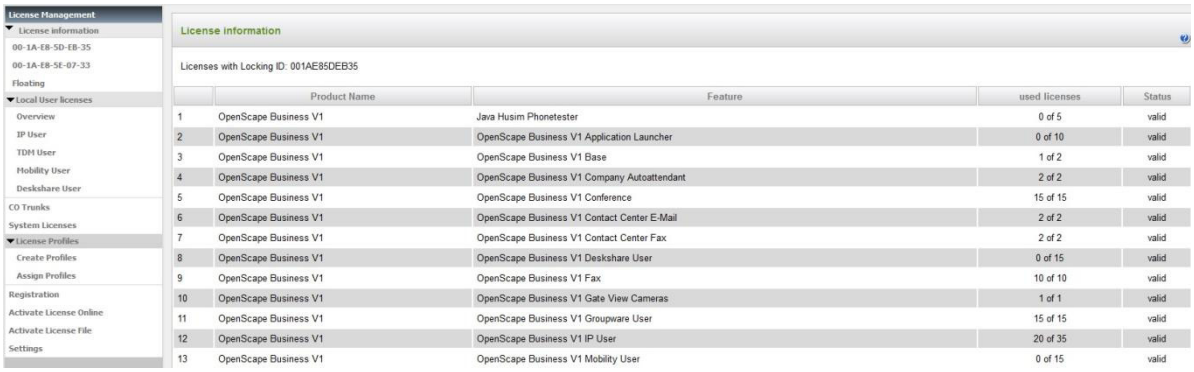
Voraussetzungen

- Das Kommunikationssystem befindet sich in einem Netzverbund.
- Sie sind am WBM angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.

2) Klicken Sie im Navigationsbaum auf **Lizenzinformationen**. Es werden Ihnen alle Lizenzen des Netzverbundes angezeigt.



	Product Name	Feature	used licenses	Status
1	OpenScape Business V1	Java Husim Phonetester	0 of 5	valid
2	OpenScape Business V1	OpenScape Business V1 Application Launcher	0 of 10	valid
3	OpenScape Business V1	OpenScape Business V1 Base	1 of 2	valid
4	OpenScape Business V1	OpenScape Business V1 Company Autoattendant	2 of 2	valid
5	OpenScape Business V1	OpenScape Business V1 Conference	15 of 15	valid
6	OpenScape Business V1	OpenScape Business V1 Contact Center E-Mail	2 of 2	valid
7	OpenScape Business V1	OpenScape Business V1 Contact Center Fax	2 of 2	valid
8	OpenScape Business V1	OpenScape Business V1 Deskshare User	0 of 15	valid
9	OpenScape Business V1	OpenScape Business V1 Fax	10 of 10	valid
10	OpenScape Business V1	OpenScape Business V1 Gate View Cameras	1 of 1	valid
11	OpenScape Business V1	OpenScape Business V1 Groupware User	15 of 15	valid
12	OpenScape Business V1	OpenScape Business V1 IP User	20 of 35	valid
13	OpenScape Business V1	OpenScape Business V1 Mobility User	0 of 15	valid

7.5.2.2 Wie Sie die an einen Knoten gebundenen Lizenzen anzeigen

Voraussetzungen

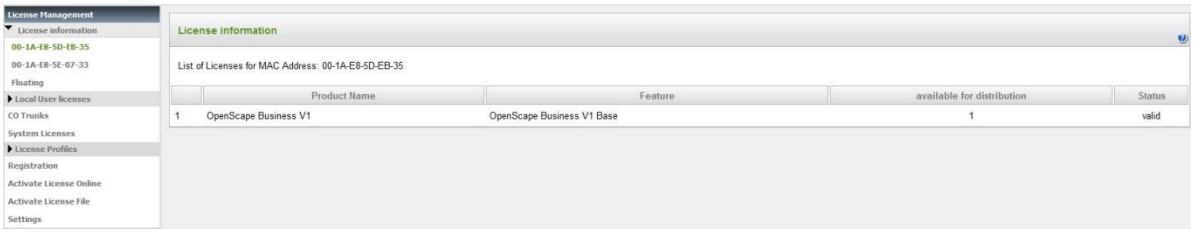
- Das Kommunikationssystem befindet sich in einem Netzverbund.
- Sie sind am WBM angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.

2) Klicken Sie im Navigationsbaum auf **Lizenzinformationen**.

3) Klicken Sie im Navigationsbaum auf den Systemnamen oder die Locking ID des gewünschten Knotens. Es werden Ihnen die speziell an diesen Knoten gebundenen Lizenzen angezeigt, wie z. B. die Basislizenz.



7.5.2.3 Wie Sie alle im Netzverbund gemeinsam genutzten Lizenzen anzeigen

Voraussetzungen

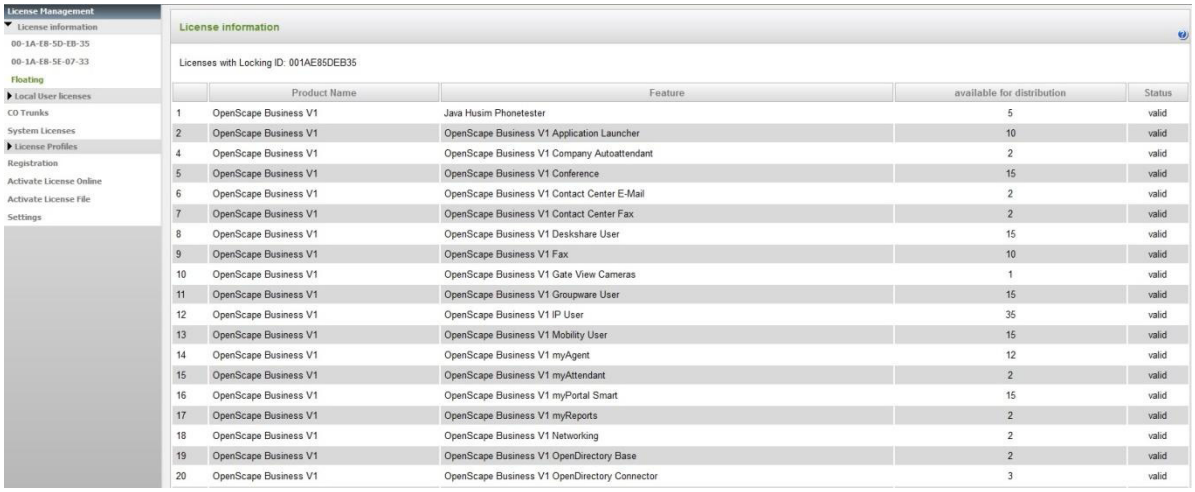
- Das Kommunikationssystem befindet sich in einem Netzverbund.
- Sie sind am WBM angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.

2) Klicken Sie im Navigationsbaum auf **Lizenzinformationen**.

3) Klicken Sie im Navigationsbaum auf **Floating**. Es werden Ihnen alle gemeinsam genutzten Lizenzen im Netzverbund angezeigt.



	Product Name	Feature	available for distribution	Status
1	OpenScape Business V1	Java Husim Phonetester	5	valid
2	OpenScape Business V1	OpenScape Business V1 Application Launcher	10	valid
4	OpenScape Business V1	OpenScape Business V1 Company Autoattendant	2	valid
5	OpenScape Business V1	OpenScape Business V1 Conference	15	valid
6	OpenScape Business V1	OpenScape Business V1 Contact Center E-Mail	2	valid
7	OpenScape Business V1	OpenScape Business V1 Contact Center Fax	2	valid
8	OpenScape Business V1	OpenScape Business V1 Deskshare User	15	valid
9	OpenScape Business V1	OpenScape Business V1 Fax	10	valid
10	OpenScape Business V1	OpenScape Business V1 Gate View Cameras	1	valid
11	OpenScape Business V1	OpenScape Business V1 Groupware User	15	valid
12	OpenScape Business V1	OpenScape Business V1 IP User	35	valid
13	OpenScape Business V1	OpenScape Business V1 Mobility User	15	valid
14	OpenScape Business V1	OpenScape Business V1 myAgent	12	valid
15	OpenScape Business V1	OpenScape Business V1 myAttendant	2	valid
16	OpenScape Business V1	OpenScape Business V1 myPortal Smart	15	valid
17	OpenScape Business V1	OpenScape Business V1 myReports	2	valid
18	OpenScape Business V1	OpenScape Business V1 Networking	2	valid
19	OpenScape Business V1	OpenScape Business V1 OpenDirectory Base	2	valid
20	OpenScape Business V1	OpenScape Business V1 OpenDirectory Connector	3	valid

7.5.2.4 Wie Sie Teilnehmer- und User-orientierte Lizenzen knotenabhängig anzeigen

Voraussetzungen

- Das Kommunikationssystem befindet sich in einem Netzverbund.
- Sie sind am WBM angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.

2) Klicken Sie im Navigationsbaum auf **Netzweite Lizenzübersicht**. Es werden Ihnen alle Teilnehmer-Lizenzen und User-orientierten Lizenzen im Netzverbund nach Knoten sortiert angezeigt.

7.6 Lizenzprofilzuordnung

Lizenzprofile enthalten vordefinierte Lizenzzuordnungen und können einem oder mehreren Teilnehmern zugewiesen werden. Lizenzprofile sind nützlich, wenn mehrere Teilnehmer dieselben Lizenzen bekommen sollen.

Es können vordefinierte Lizenzprofile verwendet oder neue Lizenzprofile erstellt werden.

Ein Lizenzprofil gilt immer für einen Teilnehmer-Typ und kann nur Teilnehmern dieses Typs zugeordnet werden. Es können mehrere Lizenzprofile für einen Teilnehmer-Typ angelegt und benannt werden.

Für folgende Teilnehmer-Typen können Lizenzprofile erstellt werden:

- IP-Teilnehmer (IP-Systemtelefone, SIP-Telefone)
- TDM-Teilnehmer (UP0-Telefone, ISDN-Telefone, analoge Telefone, DECT-Telefone)
- DeskSharing-Teilnehmer

- Mobiler Teilnehmer

Innerhalb eines Lizenzprofils können Sie dem Teilnehmer-Typ nach Ihren Wünschen userorientierte Lizenzen zuordnen.

Wird die Lizenzzuordnung eines Teilnehmers eines Lizenzprofils separat geändert, wird die Zuordnung des Teilnehmers zum Lizenzprofil automatisch aufgehoben.

7.6.1 Wie Sie ein Lizenzprofil hinzufügen

Erstellen Sie ein neues Lizenzprofil.

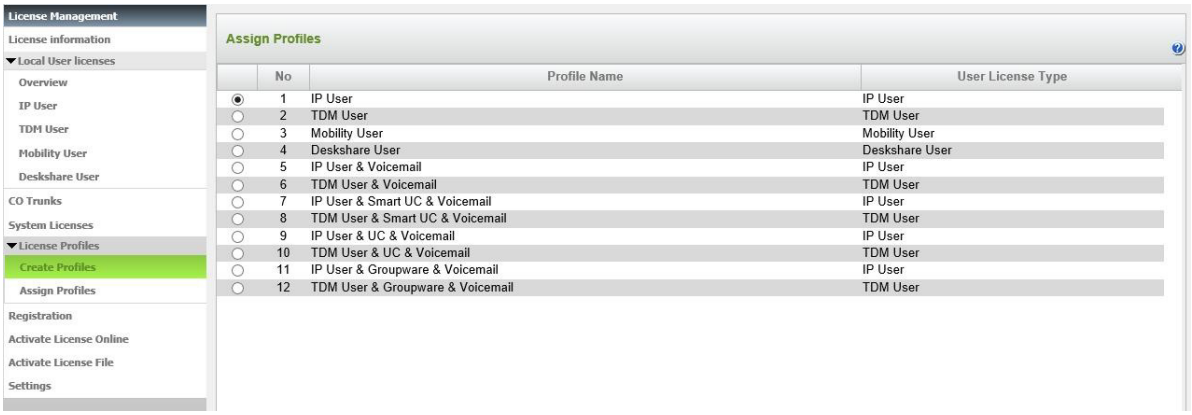
Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

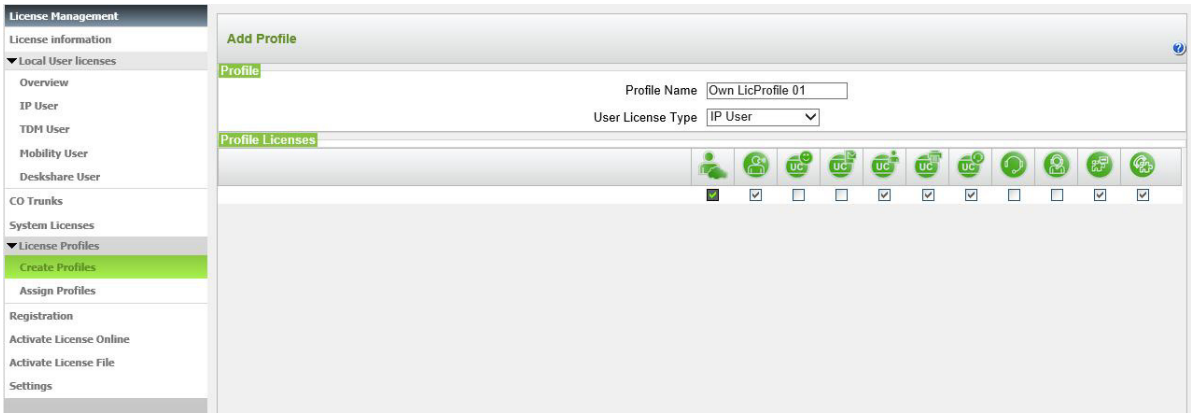
Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.

2) Klicken Sie im Navigationsbaum auf **Lizenzprofile > Profile erstellen**. Es werden Ihnen alle vorhandenen Lizenzprofile angezeigt.



3) Klicken Sie auf **Hinzufügen**.



4) Geben Sie im Feld **Profilname** einen Namen Ihrer Wahl für das neue Profil ein.

5) Wählen Sie aus der Aufklappliste **Lizenztyp Benutzer** den Teilnehmer-Typ aus, für den das Profil gelten soll.

6) Wählen Sie die User-orientierten Lizenzen, indem Sie die gewünschten Kontrollkästchen aktivieren.

7) Klicken Sie auf **OK & Weiter**. Ihre Zuordnung wird auf Richtigkeit geprüft.

   Bei fehlerfreier Zuordnung ist die Lizenzierung der Teilnehmer beendet.

8) Bei fehlerhafter Zuordnung werden Ihnen die Fehler mit einem rot hinterlegten Kontrollkästchen angezeigt. Korrigieren Sie diese Fehler und wiederholen Sie Schritt 7.

7.6.2 Wie Sie ein Lizenzprofil bearbeiten

Bearbeiten Sie ein bestehendes Lizenzprofil.

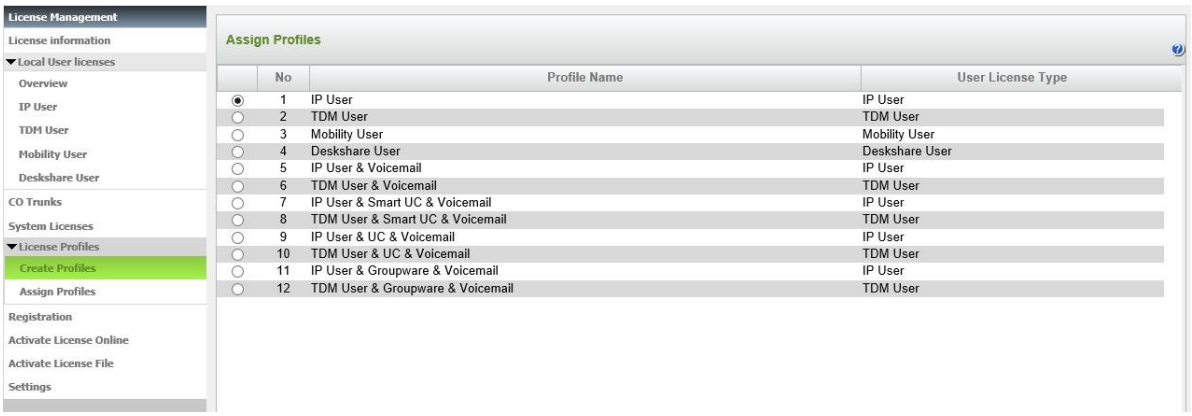
Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

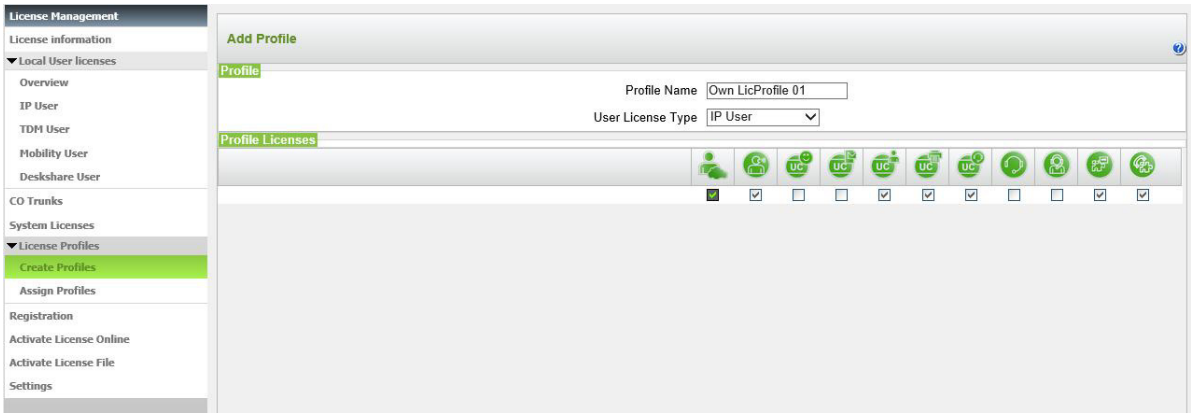
Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.

2) Klicken Sie im Navigationsbaum auf **Lizenzprofile > Profile erstellen**. Es werden Ihnen alle vorhandenen Lizenzprofile angezeigt.



3) Aktivieren Sie das Optionsfeld vor dem gewünschten Lizenzprofil und klicken Sie auf **Bearbeiten**.



4) Ändern Sie das Lizenzprofil wie gewünscht.

5) Klicken Sie auf **OK & Weiter**. Ihre Zuordnung wird auf Richtigkeit geprüft.

Bei fehlerfreier Zuordnung ist die Bearbeitung des Lizenzprofils beendet.

6) Bei fehlerhafter Zuordnung werden Ihnen die Fehler mit einem rot hinterlegten Kontrollkästchen angezeigt. Korrigieren Sie diese Fehler und wiederholen Sie Schritt 5.

7.6.3 Wie Sie Teilnehmern ein Lizenzprofil zuordnen

Ordnen Sie ein Lizenzprofil den verfügbaren Teilnehmern zu.

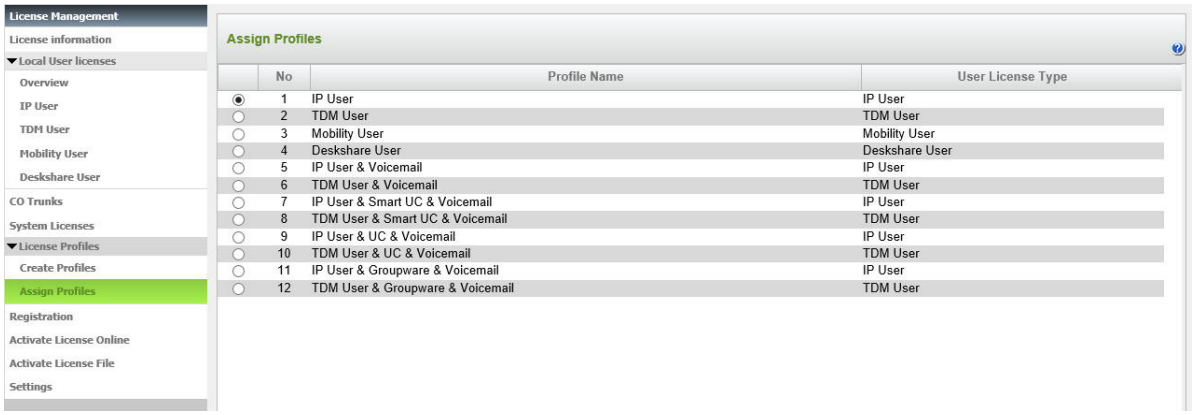
Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

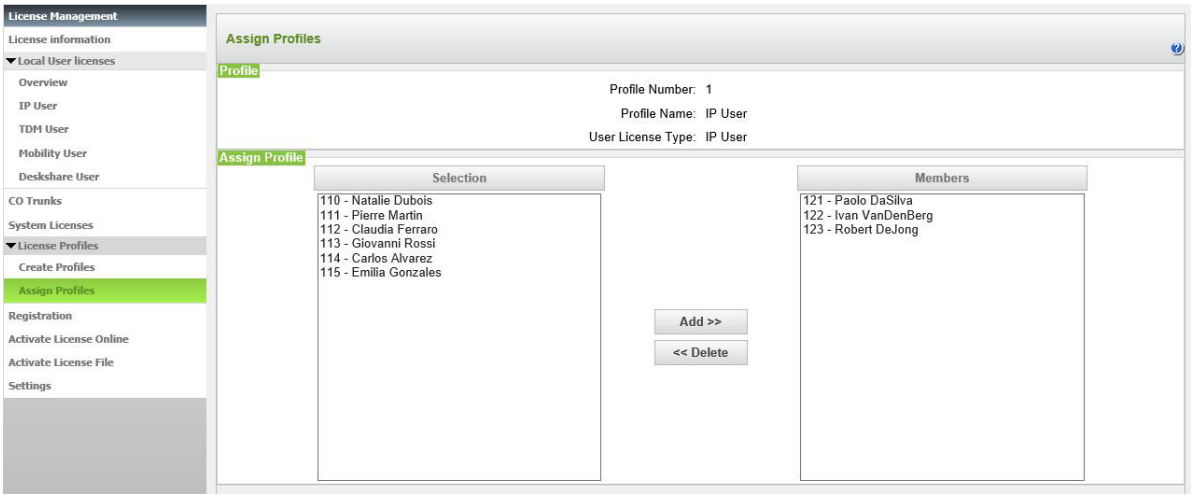
Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.

2) Klicken Sie im Navigationsbaum auf **Lizenzprofile > Profile zuweisen**. Es werden Ihnen alle vorhandenen Lizenzprofile angezeigt.



3) Aktivieren Sie das Optionsfeld vor dem gewünschten Lizenzprofil und klicken Sie auf **OK & Weiter**.



4) Markieren Sie im linken Feld **Auswahl** alle Teilnehmer, denen das Lizenzprofil zugewiesen werden soll.

5) Klicken Sie auf **Hinzufügen**. Die ausgewählten Teilnehmer erscheinen im rechten Fenster **Mitglieder**.

6) Klicken Sie auf **OK & Weiter**. Die im Lizenzprofil ausgewählten Lizenzen werden den Teilnehmern zugeordnet.

INFO: Teilnehmer können auch nachträglich aus einem Lizenzprofil entfernt oder neue Teilnehmer hinzugefügt werden.

7.6.4 Wie Sie ein Lizenzprofil löschen

Löschen Sie ein bestehendes Lizenzprofil.

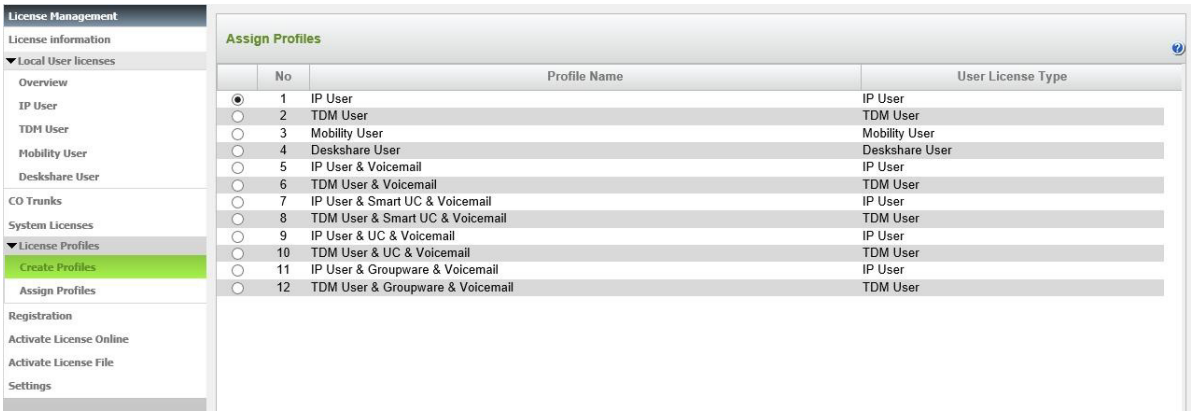
Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.

2) Klicken Sie im Navigationsbaum auf **Lizenzprofile > Profile erstellen**. Es werden Ihnen alle vorhandenen Lizenzprofile angezeigt.



3) Aktivieren Sie das Optionsfeld vor dem gewünschten Lizenzprofil und klicken Sie auf **Löschen**.

4) Bestätigen Sie den Hinweis mit **OK**. Das Lizenzprofil ist gelöscht.

7.7 Rehost nach Hardwaretausch

Lizenzen müssen aktualisiert werden, wenn am Kommunikationssystem Hardware auszutauschen ist, die eine MAC-Adresse besitzt (z. B. Mainboard der Hardware-Plattform oder Netzwerkkarte des Linux-Servers). Für den Rehost werden die MAC-Adresse der alten Hardware, die MAC-Adresse der neuen Hardware und die Anmeldedaten für den zentralen Lizenzserver (CLS) benötigt.

Nach Austausch der Hardware müssen die Konfigurationsdaten mit Hilfe des aktuellen Backup-Sets wiederhergestellt werden (siehe *Wiederherstellen*).

Da die Lizenzen an die MAC-Adresse der Hardware gebunden sind, ändert sich nach Austausch der Hardware die MAC-Adresse und somit sind die Lizenzen nicht mehr gültig. Nach Hardwaretausch befindet sich das Kommunikationssystem wieder in der Activation Period. Nachdem alte und neue MAC-Adresse am CLS eingetragen wurden, kann die neue Lizenzdatei generiert werden. Diese wird per Offline-Aktualisierung in das Kommunikationssystem geladen und anschließend werden alle vorhandenen Lizenzen automatisch aktiviert.

Für den Soft Switch wird die MAC-Adresse der Netzwerkkarte des Linux-Servers verwendet, die bei der Installation des Linux-Betriebssystems ausgewählt wurde (sichtbar über YaST). Die MAC-Adresse kann auch mit Hilfe des WBMs ausgelesen werden.

INFO: Jeder Rehost wird im CLS protokolliert. Eine Lizenz kann maximal dreimal für einen Rehost verwendet werden.

INFO: Die IP-Adresse des CLS kann über das WBM unter **Lizenzverwaltung > Einstellungen** abgefragt und falls nötig geändert werden.

7.7.1 Wie Sie einen Rehost nach einem Hardwaretausch ausführen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.
- Die Hardware ist getauscht worden und Sie haben am CLS einen Rehost durchgeführt.
- Die Konfigurationsdaten wurde mit Hilfe des aktuellen Backup-Sets wiederhergestellt.
- Sie kennen den Lizenz-Autorisierungscode (LAC) für die Lizenzfreischaltung.
- Für die Verbindung zum Lizenzserver muss das Kommunikationssystem eine Verbindung zum Internet haben.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.

2) Klicken Sie im Navigationsbaum auf **Lizenz Online aktivieren**.

3) Geben Sie im Feld **Lizenz Autorisierungs Code (LAC)** den LAC ein.

4) Lassen Sie das Kontrollkästchen für den Zugang zum Lizenzserver über Benutzername und Kennwort deaktiviert. Der Zugang zum Lizenzserver erfolgt automatisch. (Die Eingabe von Benutzername und Kennwort ist nur für Vertriebspartner nötig.)

5) Klicken Sie auf **Aktivieren**. Die Verbindung zum Lizenzserver wird hergestellt und die Lizenzen aktualisiert. Nach erfolgreicher Aktualisierung wird die Verbindung automatisch wieder abgebaut.

6) Starten Sie das Kommunikationssystem neu.

Nächste Schritte

Speichern Sie Ihre Konfigurationsdaten in einem neuen Backup-Set (siehe *Sofortiges Sichern*).

7.8 Lizenzserver (Central License Server, CLS)

Der Lizenzserver (CLS) erzeugt und verwaltet die Lizenzdateien.

Eine Lizenzdatei wird generiert, wenn der Kunde über das WBM den Lizenz-Autorisierungscode an den CLS sendet. Die Übertragung der Lizenzdatei an das Kommunikationssystem erfolgt automatisch über das Internet. Ist eine automatische Übertragung nicht möglich, kann die Lizenzdatei auch manuell in das Kommunikationssystem geladen werden.

7.8.1 Wie Sie die IP-Adresse des Lizenzservers abfragen oder ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.
- Hat sich die IP-Adresse des zentralen Lizenzservers geändert, müssen Sie die aktuelle IP-Adresse wissen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.

2) Klicken Sie im Navigationsbaum auf **Einstellungen**. Es wird Ihnen im Feld **IP-Adresse des zentralen Lizenzservers** die IP-Adresse des zentralen Lizenzservers (CLS) angezeigt. Die aktuell gültige IP-Adresse lautet `188.64.16.4`.

3) Wenn Sie die IP-Adresse des zentralen Lizenzservers ändern müssen, geben Sie im Feld **IP-Adresse des zentralen Lizenzservers** die neue IP-Adresse des zentralen Lizenzservers in der Form `123.124.125.126` ein.

4) Klicken Sie auf **Aktivieren**.

7.9 Lizenzagent (Customer License Agent, CLA)

Der Lizenzagent (CLA) ist Teil der OpenScape Business Kommunikationssoftware und läuft automatisch im Hintergrund. Er verwaltet die Lizenzdatei und die darin enthaltenen Lizenzen. Der CLA prüft die Lizenzanforderungen und schaltet bei genügend vorhandenen Lizenzen die Lizenzen frei. Pro Kommunikationssystem gibt es nur einen CLA (lokaler CLA). Sind mehrere Kommunikationssysteme (Knoten) in einem Netzverbund, sollte nur ein CLA (zentraler CLA) auf dem Master-Knoten verwendet werden.

Folgende Konfigurationen sind möglich:

- **Verbindung zum lokalen Lizenzagenten konfigurieren**
  Wird ein Knoten aus dem Netzverbund genommen, wird die Verbindung zum zentralen CLA aufgehoben. Es wird automatisch der auf dem Knoten installierte lokale CLA genutzt. Funktioniert dieser Automatismus nicht, kann die Verbindung zum lokalen CLa manuell hergestellt werden.
- **Verbindung zum zentralen Lizenzagenten ändern**
  Jeder Knoten im Netzverbund benötigt die Verbindung zum zentralen CLA auf dem Master-Knoten. Diese Verbindung wird beim Durchlaufen des WBM-Wizards **Vernetzung** automatisch hergestellt. Ändert sich die IP-Adresse des Master-Knotens, ist an allen Slave-Knoten die Verbindung zum zentralen CLA neu zu konfigurieren.

7.9.1 Wie Sie eine Verbindung zum lokalen Lizenzagenten konfigurieren

Voraussetzungen

- Sie sind am WBM des gewünschten Knotens angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.
2) Klicken Sie im Navigationsbaum auf **Einstellungen**.
3) Aktivieren Sie das Optionsfeld **Lokaler Lizenzagent (CLA)**.
4) Klicken Sie auf **Aktivieren**.

7.9.2 Wie Sie die Verbindung zum zentralen Lizenzagenten ändern

Voraussetzungen

- Das Kommunikationssystem befindet sich in einem Netzverbund.
- Sie sind am WBM des gewünschten Knotens angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.
2) Klicken Sie im Navigationsbaum auf **Einstellungen**.
3) Aktivieren Sie das Optionsfeld **Zentraler Lizenzagent** und geben Sie unter **IP-Adresse des zentralen Lizenzagenten** die IP-Adresse des Master-Knotens (Knoten 1) in der Form `123.124.125.126` ein.
4) Klicken Sie auf **Aktivieren**.

7.10 Locking ID und Advanced Locking ID

Jedem Kommunikationssystem ist eine Locking ID oder eine Advanced Locking ID zugeordnet. Um eine eindeutige Lizenzierung zu gewährleisten, werden die Lizenzen an diese Locking IDs gebunden.

Locking ID

Bei Hardware-Plattformen ist die Locking ID die MAC-Adresse des Kommunikationssystems.

Bei einem Soft Switch ist die Locking ID die MAC-Adresse der Netzwerkkarte des Linux-Servers. Enthält der Linux-Server mehrere Netzwerkkarten, ist die Netzwerkkarte auszuwählen, die bei der Erstinbetriebnahme des Linux-Servers verwendet wurde.

Befindet sich das Kommunikationssystem in der Activation Period, wird unter den Lizenzinformationen evtl. eine falsche MAC-Adresse angezeigt. Die richtige MAC-Adresse kann über das **Service-Center** unter **Inventory** abgefragt werden.

Advanced Locking ID

Läuft ein Soft Switch in einer virtuellen Umgebung, wird anstelle der Locking ID die Advanced Locking ID (ALI) verwendet. Die Advanced Locking ID wird am CLS mittels ALI-Calculator generiert.

Folgende System- und Netzwerkparameter müssen konfiguriert sein, da sie für die Generierung der 24-stelligen Advanced Locking ID verwendet werden:

- IP-Adresse des Default-Gateways (Linux-Server)
- Hostname des Linux-Servers
- IP-Adresse des Linux-Servers
- IP-Adresse des DNS-Servers (konfiguriert im Linux-Server)
- Zeitzone (Linux-Server)

Sind einer oder mehrere dieser System- und Netzwerkparameter nicht eingerichtet, so kann die Advanced Locking ID nicht generiert werden.

Die Advanced Locking ID wird im WBM angezeigt. In einigen Fällen ist es möglich, dass die ALI, die am CLS für die Lizenzdatei generiert wurde, abweicht von der ALI, die während der Activation Period im WBM angezeigt wird. Die Lizenzdatei mit der abweichenden ALI wird vom System trotzdem akzeptiert.

Ändert sich einer der oben aufgeführten System- und Netzwerkparameter fällt der Soft Switch zurück in die Restlaufzeit der Activation Period und eine neue Advanced Locking ID wird generiert. Um die gekaufte Lizenzdatei wieder nutzen zu können, muss am Zentralen Lizenzserver (CLS) ein Rehost von der alten auf die neue Advanced Locking ID durchgeführt werden.

7.10.1 Wie Sie die Locking ID des Kommunikationssystems abfragen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Inventory**. Es wird Ihnen eine Übersicht der Komponenten angezeigt, die zum Kommunikationssystem gehören.

3) Klicken Sie auf **OK & Weiter**. Es werden Ihnen Informationen über die Hardware und die Software angezeigt. Unter **MAC-ID für Lizenz** finden Sie die Locking ID des Kommunikationssystems.

7.10.2 Wie Sie die Locking ID des Soft Switches abfragen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Inventory**. Es werden Ihnen Informationen über die Software des Soft Switches, über den verfügbaren und den belegten Speicher der Festplatten und über den Applikationsstatus angezeigt. Unter **MAC-ID für Lizenz** finden Sie die Locking ID des Soft Switches.

7.10.3 Wie Sie die Advanced Locking ID des Soft Switches abfragen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

› Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**. Es werden Ihnen alle vorhandenen Lizenzen angezeigt. Unter **Locking ID** finden Sie die Advanced Locking ID des Soft Switches, wenn der Soft Switch in einer virtualisierten Umgebung betrieben wird.

8 Integration ins interne Datennetz (LAN)

Die Integration des Kommunikationssystems in das bestehende interne Datennetz (LAN) ermöglicht die Nutzung der UC-Lösungen und der Administration des Kommunikationssystems über PCs im internen Netz.

Folgende Netzwerkparameter sind im WBM einzurichten:

- Hardware-Plattform OpenScape Business X: IP-Adresse und Netzmaske des Mainboards und der UC Booster Card (falls vorhanden). Diese Einstellungen werden während der Erstinstallation getroffen, können aber nachträglich geändert werden.
  Softswitch OpenScape Business S: IP-Adresse und Netzmaske des Linux-Servers, auf dem die Kommunikationssoftware läuft. Diese Einstellungen werden während der Linux-Installation getroffen, können aber nachträglich geändert werden.
- Das Kommunikationssystem kann optional als DHCP-Server (mit Versorgung von netzwerkspezifischen Parametern wie Netzmaske, Default Gateway, DNS-Server) oder als DHCP Relay Agent eingerichtet werden. Die Einrichtung als DHCP-Server wird während der Erstinstallation getroffen, kann aber nachträglich geändert werden. Die Einrichtung als DHCP Relay Agent erfolgt über den Experten-Modus.
- IP-Adresse des Default Routers und des (externen) DNS-Servers für den Zugang zu anderen IP-Netzen (z.B. Internet). Diese Einstellungen werden während der Erstinstallation getroffen, können aber nachträglich geändert werden.

8.1 LAN-Schnittstelle

Um das Kommunikationssystem in die LAN-Infrastruktur einzubinden, müssen die IP-Adresse und der interne IP-Adressbereich des Kommunikationssystems an das IP-Adressen-Schema des internen Netzes (LAN) angepasst werden.

8.1.1 IP-Adresse und Netzmaske der LAN-Schnittstelle

IP-Adresse und Netzmaske des Kommunikationssystems werden bei der Erstinstallation definiert, können aber auch nachträglich geändert werden. Eventuell müssen IP-Adresse und/oder Netzmaske an den IP-Adressbereich des LAN angepasst werden.

Hardware-Plattform

Der Hardware-Plattform ist standardmäßig eine IP-Adresse und eine Subnetzmaske zugewiesen. Die UC Booster Card benötigt ebenfalls eine IP-Adresse. Unabhängig davon, ob sie gesteckt ist oder nicht, kann die IP-Adresse der UC Booster Card eingerichtet werden.

Die Hardware-Plattform verwendet für die Integration in das LAN die Schnittstelle "LAN" des Mainboards. Ist die UC Booster Card gesteckt, muss zusätzlich die Schnittstelle "LAN" der UC Booster Card an das LAN angeschlossen werden. Hardware-Plattform und UC Booster Card müssen sich in dem selben Subnetz befinden.

Um die Änderungen von IP-Adresse oder Netzmaske zu aktivieren, ist bei der Hardware-Plattform ein Neustart notwendig.

Die Änderungen der IP-Adresse und der Netzmaske bleiben bei einer Softwareaktualisierung erhalten, werden aber bei einem Reload der Hardware-Plattform wieder auf die Standardwerte zurückgesetzt. Diese Änderungen können nicht in einem Backup-Set gespeichert werden.

Softswitch

Beim Softswitch wird der Linux-Server, auf dem die Kommunikationssoftware läuft, über seine Netzwerkkarte in das LAN integriert.

Die Änderungen von IP-Adresse oder Netzmaske sind nach einem Restart der Applikation aktiv (siehe *Restart, Reload, Shutdown*).

8.1.1.1 Wie Sie IP-Adresse und Netzmaske der Hardware-Plattform ändern

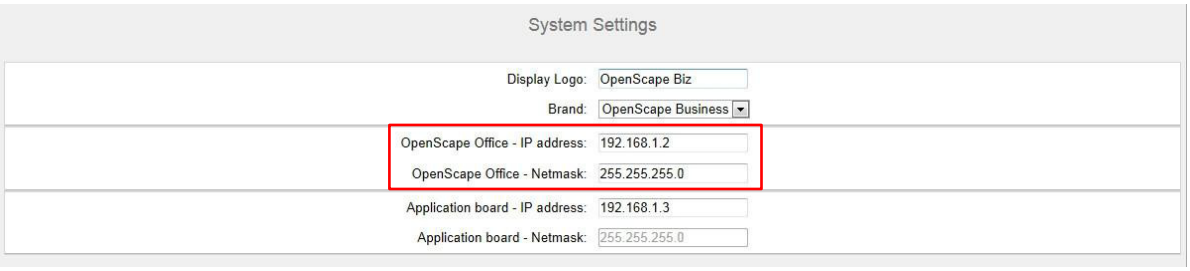
Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie auf **Bearbeiten**, um den Wizard **Erstinstallation** zu starten.



3) Ändern Sie unter **OpenScape Business - IP-Adresse** die IP-Adresse der Hardware-Plattform. Die IP-Adresse muss zu dem IP-Adressen-Schema des internen Netzes passen und darf keinem bestehenden Netzwerk-Client zugewiesen sein, da es sonst zu einem IP-Adressenkonflikt kommt. Standardmäßig ist die IP-Adresse `192.168.1.2` eingetragen.

4) Ändern Sie unter **OpenScape Business - Netzmaske** die Netzmaske der Hardware-Plattform. Die Netzmaske muss zu dem IP-Adressen-Schema des internen Netzes passen. Standardmäßig ist die Netzmaske `255.255.255.0` eingetragen.

5) Klicken Sie auf **OK & Weiter**.

6) Klicken Sie so oft auf **OK & Weiter**, bis Sie die Meldung erhalten, dass das Leistungsmerkmal eingerichtet wurde.

7) Klicken Sie auf **Beenden**. Die Hardware-Plattform führt automatisch einen Neustart durch.

8.1.1.2 Wie Sie IP-Adresse der UC Booster Card ändern

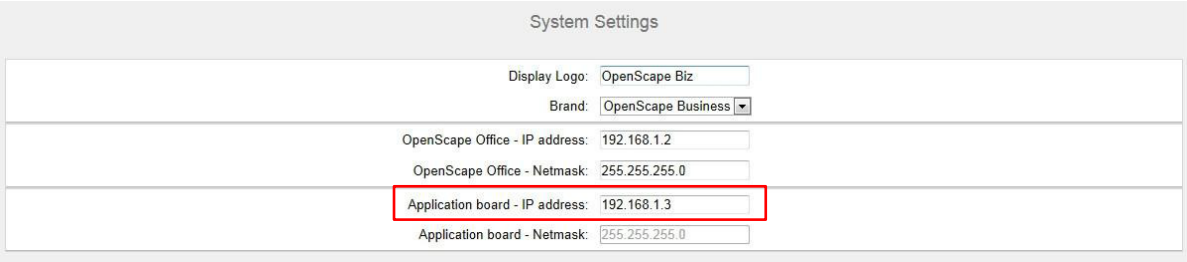
Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie auf **Bearbeiten**, um den Wizard **Erstinstallation** zu starten.



3) Ändern Sie unter **UC Booster Card - IP-Adresse** die IP-Adresse der UC Booster Card. Die IP-Adresse muss zu dem IP-Adressen-Schema des internen Netzes passen und darf keinem bestehenden Netzwerk-Client zugewiesen sein, da es sonst zu einem IP-Adressenkonflikt kommt. Standardmäßig ist die IP-Adresse `192.168.1.3` eingetragen.

4) Klicken Sie auf **OK & Weiter**.

5) Klicken Sie so oft auf **OK & Weiter**, bis Sie die Meldung erhalten, dass das Leistungsmerkmal eingerichtet wurde.

6) Klicken Sie auf **Beenden**. Die Hardware-Plattform führt automatisch einen Neustart durch.

8.1.1.3 Wie Sie IP-Adresse und Netzmaske des Softswitches ändern

Schritt für Schritt

1) Klicken Sie in der Taskleiste auf **Computer**.

2) Klicken Sie im Menübaum auf **System > YaST**.

3) Geben Sie das Passwort für den Benutzer root ein und klicken Sie auf **Continue**. Es öffnet sich das YaST Control Center.

4) Klicken Sie im Menübaum auf **Network Devices**.

5) Klicken Sie im Bereich **Network Devices** auf **Network Settings**.

6) Markieren Sie im Register **Overview** die gewünschte Netzwerkkarte und klicken Sie auf **Edit**.

7) Aktivieren Sie das Optionsfeld **Statically assigned IP Address**.

8) Ändern Sie unter **IP Address** die IP-Adresse des Linux-Servers, auf dem die Software des Softswitches läuft. Die IP-Adresse muss zu dem IP-Adressen-Schema des internen Netzes passen und darf keinem bestehenden Netzwerk-Client zugewiesen sein, da es sonst zu einem IP-Adressenkonflikt kommt.

9) Ändern Sie unter **Subnet Mask** die Subnetzmaske des Linux-Servers. Die Subnetzmaske muss zu dem IP-Adressen-Schema des internen Netzes passen.

10) Klicken Sie auf **Next** und anschließend auf **OK**.

11) Schließen Sie das **YaST Control Center**.

8.1.2 Interner IP-Adressbereich der LAN-Schnittstelle

Der interne IP-Adressbereich der LAN-Schnittstelle, den die Hardware-Plattform für die interne Kommunikation ihrer Module verwendet, kann bei Bedarf geändert werden.

Die Hardware-Plattform nutzt standardmäßig den internen IP-Adressbereich 192.168.3.xxx. Dieser kann auch auf den gewünschten IP-Adressbereich geändert werden. Die interne Subnetzmaske ist 255.255.255.0 und kann nicht geändert werden.

Um die Änderungen des internen IP-Adressbereichs zu aktivieren, ist ein Neustart der Hardware-Plattform notwendig.

Die Änderungen des internen IP-Adressbereichs bleiben bei einer Softwareaktualisierung erhalten, werden aber bei einem Reload wieder auf die Standardwerte zurückgesetzt. Diese Änderungen können nicht in einem Backup-Set gespeichert werden.

8.1.2.1 Wie Sie den internen IP-Adressbereich der Hardware-Plattform ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

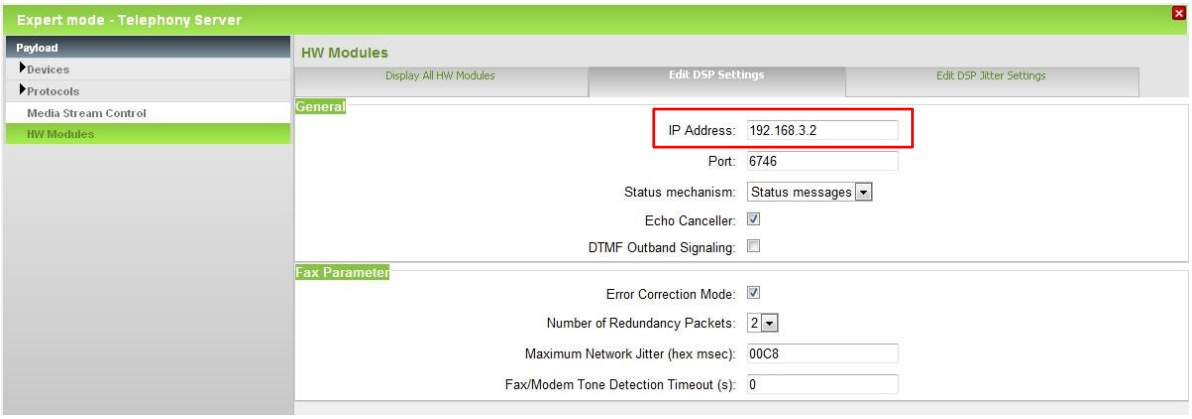
Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Payload**.

3) Klicken Sie im Menübaum auf **Hardware-Module**.

4) Klicken Sie auf die Registerkarte **DSP-Einstellungen ändern**.



5) Geben Sie im Bereich **Allgemein** unter **IP-Adresse** eine IP-Adresse für das Kommunikationssystem ein, die im gewünschten neuen internen Bereich liegt, z. B. `192.168.40.2`. Der gesamte IP-Bereich (im Beispiel `192.168.40.xxx`) ist nun für andere Clients im LAN gesperrt.

6) Klicken Sie auf **Übernehmen** und bestätigen Sie mit **OK**.

8.1.2.2 Wie Sie den internen IP-Adressbereich der Hardware-Plattform zurücksetzen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

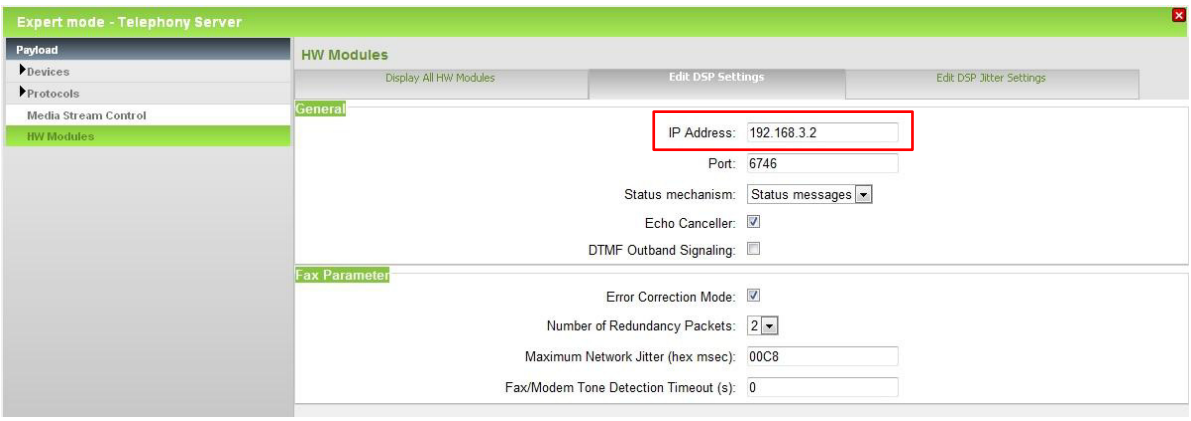
Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Payload**.

3) Klicken Sie im Menübaum auf **Hardware-Module**.

4) Klicken Sie auf die Registerkarte **DSP-Einstellungen ändern**.



5) Geben Sie im Bereich **Allgemein** unter **IP-Adresse** die IP-Adresse `192.168.3.2` ein. Der gesamte IP-Bereich `192.168.3.xxx` ist nun für andere Clients im LAN gesperrt.

6) Klicken Sie auf **Übernehmen** und bestätigen Sie mit **OK**.

8.2 DHCP

DHCP (Dynamic Host Configuration Protocol) ermöglicht mit Hilfe eines DHCP-Servers die dynamische Zuweisung von netzwerkspezifischen Daten an die IP-Teilnehmer eines Netzes (z. B. LAN).

Durch DHCP wird die automatische Integration eines IP-Teilnehmers (z. B. IP-Telefone oder PCs) in ein bestehendes LAN ermöglicht. Der IP-Teilnehmer muss für den automatischen Empfang der netzwerkspezifischen Daten eingerichtet sein und ist damit ein DHCP-Client. Der DHCP-Server versorgt den IP-Teilnehmer auf Anfrage mit den netzwerkspezifischen Daten.

8.2.1 DHCP-Relay-Agent

Bei Verwendung des internen DHCP-Servers der Hardware-Plattform müssen sich der interne DHCP-Server und die DHCP-Clients im selben Netzsegment befinden. Ist das nicht der Fall, muss die Hardware-Plattform als DHCP-Relay-Agent konfiguriert werden. Die DHCP-Anfragen der IP-Teilnehmer werden dann von der Hardware-Plattform an den eigentlichen DHCP-Server weitergeleitet.

8.2.1.1 Wie Sie die Hardware-Plattform als DHCP-Relay-Agent konfigurieren

Wird die Hardware-Plattform als DHCP-Relay-Agent konfiguriert, gibt es die DHCP-Anfragen an den externen DHCP-Server weiter.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

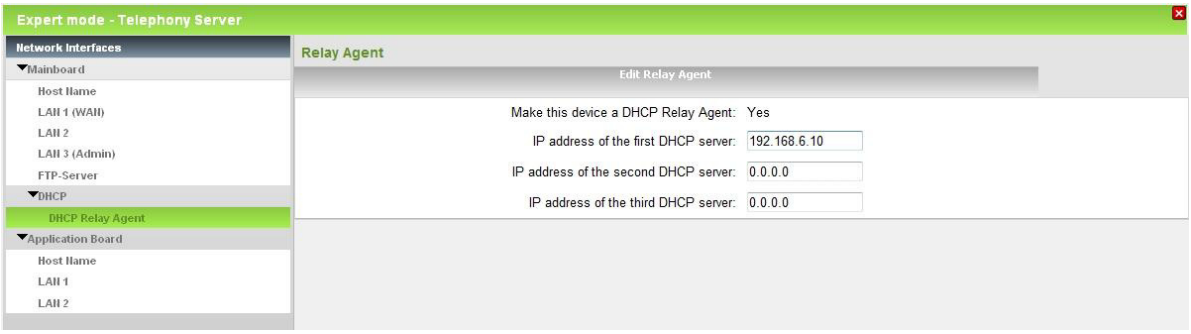
2) Klicken Sie im Navigationsbaum auf **Telefonie > Netzwerkschnittstellen**.

3) Klicken Sie im Menübaum auf **Mainboard > DHCP**.

4) Aktivieren Sie das Optionsfeld **DHCP Relay-Agent**.

5) Klicken Sie auf **Übernehmen** und bestätigen Sie mit **OK**.

6) Klicken Sie im Menübaum auf **DHCP Relay-Agent**.



7) Geben Sie die **IP-Adresse des ersten DHCP-Servers** ein.

8) Geben Sie bei Bedarf die **IP-Adresse des zweiten DHCP-Servers** ein.

9) Geben Sie bei Bedarf die **IP-Adresse des dritten DHCP-Servers** ein.

> ***INFO:*** Sie können bis zu drei DHCP-Server eingeben. Zwingend ist die Eingabe des ersten DHCP-Servers.

10) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

8.2.2 DHCP-Server

Der DHCP-Server weist den IP-Teilnehmern (IP-Telefone, SIP-Telefone, PCs, WLAN Access Points, usw.) dynamisch die netzwerkspezifischen Daten zu, wie z. B. die zu verwendende IP-Adresse und Netzmaske des IP-Teilnehmers, die IP-Adresse des Standard-Gateways, die IP-Adresse des SNTP-Servers, usw.

Als DHCP-Server kann der interne DHCP-Server des Kommunikationssystems oder ein externer DHCP-Server genutzt werden (z. B. der DHCP-Server des Internet-Routers).

Bei der Hardware-Plattform ist der integrierte DHCP-Server standardmäßig aktiviert. Soll ein externer DHCP-Server verwendet werden, muss der interne DHCP-Server deaktiviert werden. Andernfalls kommt es zu Konflikten mit dem externen DHCP-Server.

Bei dem Softswitch kann der Linux-Server als interner DHCP-Server konfiguriert werden.

Bei der Erstinbetriebnahme sollte entschieden werden, ob der interne DHCP-Server des Kommunikationssystems oder ein externer DHCP-Server genutzt werden soll. Der interne DHCP-Server kann auch nachträglich aktiviert oder deaktiviert werden. Auch die netzwerkspezifischen Daten können nachträglich konfiguriert werden.

Interner DHCP-Server

Wird der interne DHCP-Server genutzt, werden die IP-Teilnehmer automatisch mit folgenden netzwerkspezifischen Daten versorgt:

- IP-Adresse und Netzmaske des IP-Teilnehmers

- IP-Adresse des Kommunikationssystems (Default-Gateway)
- IP-Adresse des SNTP-Servers (für die Versorgung mit Datum & Uhrzeit)
- IP-Adresse des DNS-Servers (für die Namensauflösung)
- IP-Adresse des SIP-Servers (für die Authentifizierung von SIP-Teilnehmern)
- IP-Adresse des internen DLI oder des externen DLS-Servers (für die Softwareaktualisierung der IP-Systemtelefone)
- Routing-Regeln

Externer DHCP-Server

Wird ein externer DHCP-Server genutzt, muss dieser einen Vendor Specific Option Space unterstützen, der es ermöglicht, herstellerspezifische Parameter zu versorgen. Folgende netzwerkspezifischen Daten sollten im externen DHCP-Server eingegeben werden:

- IP-Adresse und Netzmaske des IP-Teilnehmers
- IP-Adresse des Default Routers = Option 3
- IP-Adresse des Kommunikationssystems (Default-Gateway) = Option 33
- IP-Adresse des DNS-Servers (für die Namensauflösung) = Option 6
- IP-Adresse des internen DLI oder des externen DLS-Servers (für die Softwareaktualisierung der IP-Systemtelefone) = Option 43
- nur für SIP-Telefone: IP-Adresse des SIP-Servers (SIP-Registrar, für die Authentifizierung von SIP-Teilnehmern) = Option 120
- nur für SIP-Telefone: IP-Adresse des SNTP-Servers (für die Versorgung der SIP-Telefone mit Datum & Uhrzeit) = Option 42

Ist eine Eingabe am externen DHCP-Server nicht möglich, so müssen diese Daten direkt an den IP-Systemtelefonen eingegeben werden. Nur dann werden die IP-Systemtelefone automatisch z. B. mit dem aktuellen Datum und Uhrzeit und mit dem neuesten Software-Update versorgt.

DHCP-Address-Pool (IP-Adressbereiche)

Meldet sich ein IP-Teilnehmer am DHCP-Server an, bekommt er u.a. eine dynamische IP-Adresse zugewiesen. Der Administrator kann einen IP-Adressbereich festlegen, aus dem der DHCP-Server die IP-Adressen an die IP-Teilnehmer vergeben darf. Es sollen z. B. nicht alle IP-Adressen aus dem Band 192.168.1.x vergeben werden, sondern nur von 192.168.1.50 bis 192.168.1.254, da die unteren IP-Adressen bis 192.168.1.49 für IP-Teilnehmer mit statischen IP-Adressen reserviert sein sollen.

Im Experten-Modus lassen sind unter **Netzwerk-Schnittstellen** für den internen DHCP-Server sogar mehrere IP-Adressbereiche einrichten.

8.2.2.1 Wie Sie den DHCP-Server der Hardware-Plattform aktivieren und konfigurieren

Mit dem Wizard **Netzwerk-Konfiguration** können Sie den internen DHCP-Server der Hardware-Plattform aktivieren und konfigurieren.

Voraussetzungen

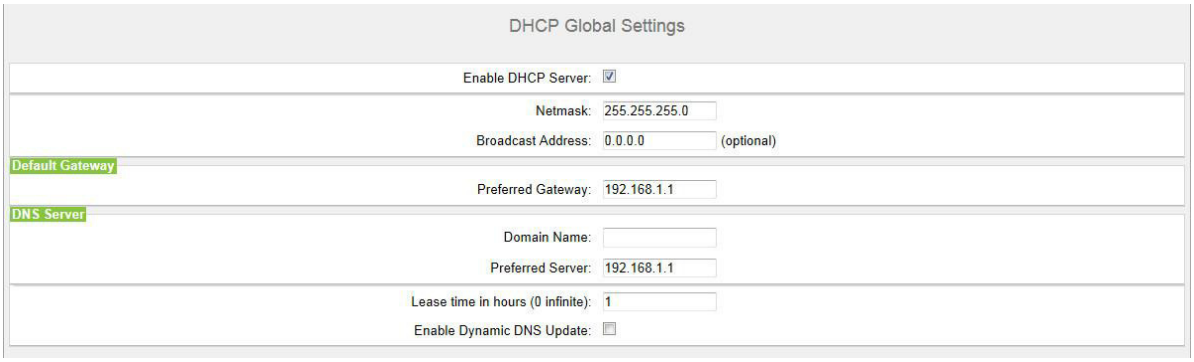
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Netzwerk/Internet**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Netzwerk-Konfiguration** zu starten.



4) Aktivieren Sie das Kontrollkästchen **DHCP-Server**.

5) Geben Sie im Feld **Netzmaske** die Netzmaske Ihres Netzwerks ein (z. B. `255.255.255.0`).

6) Geben Sie nur bei Bedarf im Feld **Broadcast-Adresse** die in diesem Netz verwendete Broadcast-Adresse ein ("letzte" IP-Adresse des Netzes bzw. des Subnetzes, Standard: `0.0.0.0`).

7) Geben Sie im Feld **Bevorzugtes Gateway** die IP-Adresse des Standardgateways ein. In der Regel ist das die IP-Adresse des Internet-Routers, z. B. `192.168.1.1`.

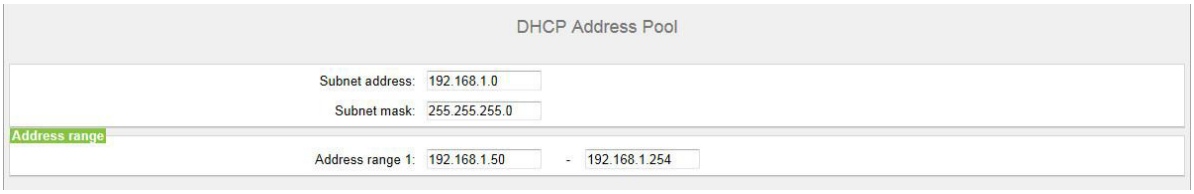
8) Wenn Sie einen vollqualifizierten Domänennamen für den DHCP-Server benötigen, geben Sie diesen unter **Domänen-Name** ein (max. 80 Zeichen).

9) Geben Sie im Feld **Bevorzugter Server** die IP-Adresse eines verfügbaren DNS-Servers ein, z. B. die IP-Adresse des Internet-Routers, `192.168.1.1`.

10) Geben Sie nur bei Bedarf im Feld **Gültigkeitsdauer in Stunden (0 unendlich)** die maximale Gültigkeitsdauer in Stunden ein (Standard: 1 h, 0 = unendliche Gültigkeitsdauer).

11) Wenn Sie ein dynamisches Update des DNS-Servers erlauben wollen, aktivieren Sie die Option **Dynamisch DNS aktualisieren** (Standard: nicht aktiviert).

12) Klicken Sie auf **OK & Weiter**. Die Einstellungen zum DHCP-Adress-Pool werden angezeigt.



13) Geben Sie im Feld **Subnetz Adresse** die unterste IP-Adresse des Subnetzes ein, in dem sich der gewünschte IP-Adressbereich befindet (im Beispiel `192.168.1.0`).

14) Geben Sie im Feld **Netzmaske** die Netzmaske des gewünschten IP-Adressbereichs ein (z. B. `255.255.255.0`).

15) Geben Sie im Feld **Adressbereich 1** die untere und obere Grenze des gewünschten IP-Adressbereichs ein (z. B. `192.168.1.50` bis `192.168.1.254`).

16) Klicken Sie auf **OK & Weiter**. Das Fenster **Routing-Einstellungen** wird angezeigt.

17) Geben Sie im Feld **IP-Adresse des DNS-Servers** die IP-Adresse eines verfügbaren DNS-Servers ein, z. B. die IP-Adresse des Internet-Routers, `192.168.1.1`.

18) Wählen Sie aus der Aufklappliste **Default-Routing über** den Eintrag **LAN** aus.

19) Wenn der Zugang zum Internet über einen Internet-Router erfolgt, geben Sie im Feld **IP-Adresse des Default-Routers** die IP-Adresse des Internet-Routers (z. B. `192.168.1.1`) ein.

20) Klicken Sie auf **OK & Weiter** und anschließend auf Beenden.

8.2.2.2 Wie Sie den DHCP-Server der Hardware-Plattform deaktivieren

Mit dem Wizard **Netzwerk-Konfiguration** können Sie den internen DHCP-Server der Hardware-Plattform deaktivieren.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Netzwerk/Internet**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Netzwerk-Konfiguration** zu starten.

4) Deaktivieren Sie das Kontrollkästchen **DCHP-Server aktivieren**.

5) Klicken Sie so oft auf **OK & Weiter**, bis Sie die Meldung erhalten, dass das Leistungsmerkmal eingerichtet wurde.

6) Klicken Sie auf **Beenden**.

8.2.2.3 Wie Sie den DHCP-Server des Softswitches aktivieren und konfigurieren

Schritt für Schritt

1) Klicken Sie in der Taskleiste auf **Computer**.

2) Klicken Sie im Menübaum auf **System > YaST**.

3) Geben Sie das Passwort für den Benutzer root ein und klicken Sie auf **Continue**. Es öffnet sich das YaST Control Center.

4) Klicken Sie im Menübaum auf **Network Services**.

5) Klicken Sie im Bereich **Network Services** auf **DHCP Server**.

6) Markieren Sie die gewünschte Netzwerkkarte und klicken Sie auf **Select**.

7) Aktivieren Sie das Kontrollkästchen **Open Firewall for Selected Interfaces**.

8) Klicken Sie auf **Next**.

9) Wenn Sie einen vollqualifizierten Domänennamen für den DHCP-Server benötigen, geben Sie diesen unter **Domain Name** ein (max. 80 Zeichen).

10) Geben Sie im Feld **Primary Name Server IP** die IP-Adresse eines verfügbaren DNS-Servers ein, z. B. die IP-Adresse des Internet-Routers, `192.168.1.1`.

11) Geben Sie im Feld **Default Gateway (Router)** die IP-Adresse des Standardgateways ein. In der Regel ist das die IP-Adresse des Internet-Routers, z. B. `192.168.1.1`.

12) Geben Sie im Feld **NTP Time Server** den bei der Erstinbetriebnahme festgelegten SNTP-Server ein.

13) Klicken Sie auf **Next**.

14) Geben Sie im Feld **First IP Address** die untere Grenze und im Feld **Last IP Address** die obere Grenze des gewünschten IP-Adressbereichs ein (z. B. `192.168.1.50` bis `192.168.1.254`).

15) Aktivieren Sie das Kontrollkästchen **Allow Dynamic BOOTP**.

16) Klicken Sie auf **Next**.

17) Aktivieren Sie das Optionsfeld **When Booting**.

18) Klicken Sie auf **Finish**.

19) Schließen Sie das **YaST Control Center**.

8.2.2.4 Wie Sie den DHCP-Server des Softswitches deaktivieren

Schritt für Schritt

1) Klicken Sie in der Taskleiste auf **Computer**.
2) Klicken Sie im Menübaum auf **System > YaST**.
3) Geben Sie das Passwort für den Benutzer root ein und klicken Sie auf **Continue**. Es öffnet sich das YaST Control Center.
4) Klicken Sie im Menübaum auf **Network Services**.
5) Klicken Sie im Bereich **Network Services** auf **DHCP Server**.
6) Deaktivieren Sie das Kontrollkästchen **Start DHCP Server**.
7) Klicken Sie auf **Finish**.
8) Schließen Sie das **YaST Control Center**.

8.3 DNS - Namensauflösung

Der Domain Name Service (DNS) dient der Umsetzung von Namen in numerische Adressen. Damit können Rechnernamen oder Domänen-Namen in IP-Adressen übersetzt werden und umgekehrt.

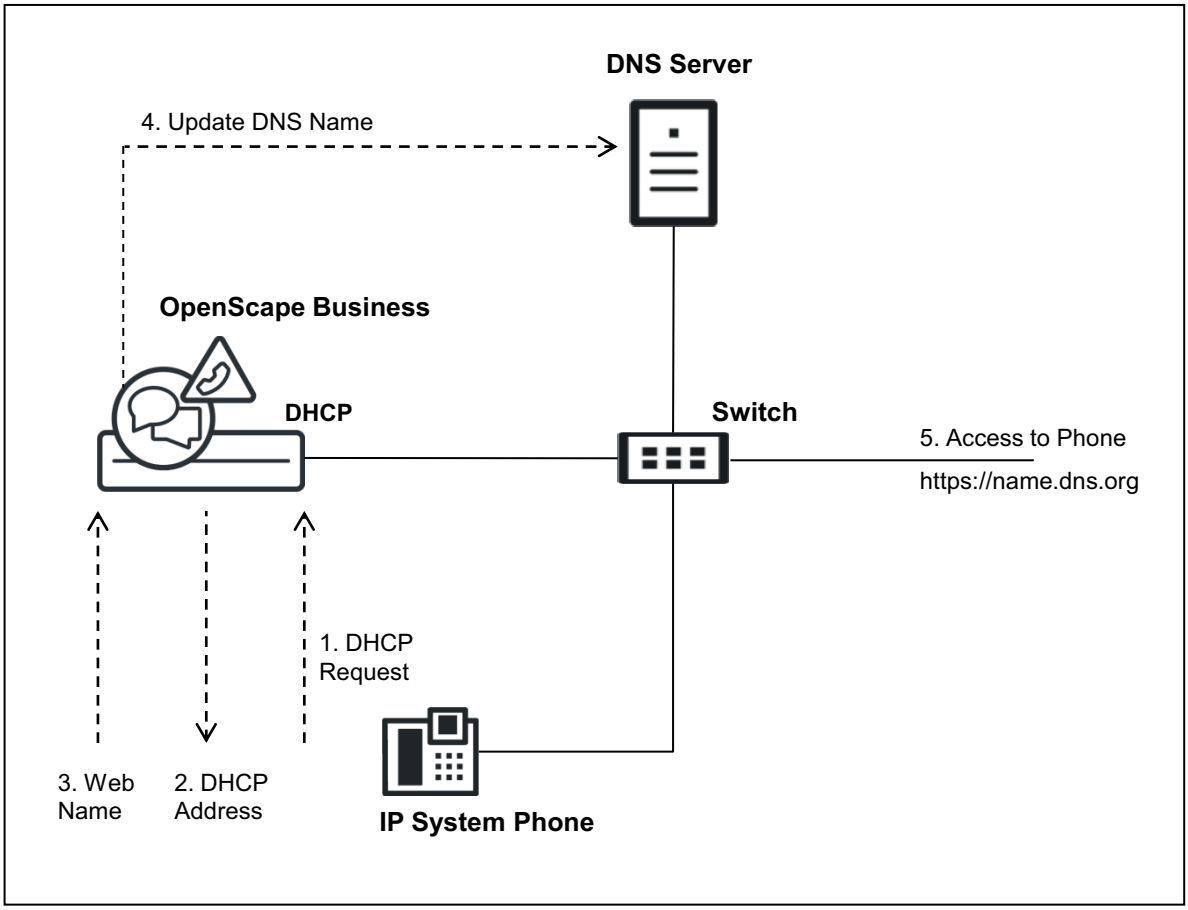
DNS nutzt eine weltweit auf Servern verteilte hierarchische Datenbank, die den Namensraum des Internets verwaltet. Dieser Namensraum ist in so genannte Zonen (Domänen) unterteilt. Für lokale Anforderungen – etwa innerhalb eines Firmennetzes – werden in der Regel eigene DNS-Server betrieben, die vom Internet unabhängig sind.

Namensauflösung bei IP-Systemtelefonen

Folgende Voraussetzungen müssen erfüllt sein:

- Windows 2008 DNS-Server (mit aktuellem Patchstand und die Einstellung "unsicheren Update zulassen" muss aktiviert werden)
- Interner DHCP-Server ist aktiviert
- Die Funktionalität "Dynamisch DNS aktualisieren" ist im internen DHCP-Server aktiviert (siehe *DHCP-Server*)
- Im IP-Systemtelefon ist der Web-Name eingetragen.

Das IP-Systemtelefon sendet einen DHCP-Request (1) und erhält vom internen DHCP-Server eine gültige IP-Adresse und die weiteren netzwerkspezifischen Daten (2). Nach dem Erhalt dieser Daten sendet das IP-Systemtelefon den eingestellten Web-Namen an den internen DHCP-Server (3), der den Namen automatisch an den konfigurierten DNS-Server weiterleitet (4). Der DNS-Server kennt nun den zur IP-Adresse des IP-Systemtelefons gehörenden Namen. Das IP-Systemtelefon kann nun z. B. über das WBM mit seinem Web-Namen angesprochen werden (5).



DNS-Server

Der DNS-Server, auch Nameserver genannt, ist ein Programm, das Anfragen zu Domänen-Namen oder Rechnernamen beantwortet. Auch der PC, auf dem dieses Programm läuft, kann als DNS-Server bezeichnet werden.

Bei Anfragen nach einem Domänen-Namen oder einem Rechnernamen sendet der DNS-Server die zugehörige IP-Adresse.

Beispiel: Für `www.wikipedia.org` geben die DNS-Server im Internet die IP-Adresse `91.198.174.2` zurück.

Kann der bevorzugte DNS-Server die Anfrage nicht beantworten, leitet er diese an einen anderen DNS-Server weiter.

Beim Softswitch kann der Linux-Server, auf dem die Kommunikationssoftware läuft, als DNS-Server konfiguriert werden. Die Hardware-Plattform kann nicht als DNS-Server eingesetzt werden. Sowohl beim Softswitch als auch bei der Hardware.Plattform kann ein externer DNS-Server angegeben werden.

8.3.1 Wie Sie einen externen DNS-Server festlegen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Routing**.

3) Navigieren Sie im Menübaum zu **IP-Routing > Mainboard > DNS-Server**. Das Fenster **DNS-Einstellungen ändern** erscheint.



4) Geben Sie im Feld **IP-Adresse des DNS-Servers** die IP-Adresse des gewünschten externen DNS-Servers ein.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

8.4 IP-Routing

IP-Routing bezeichnet in der Datentechnik das Festlegen von Wegen (Routen) für Datenströme innerhalb von Netzwerken. IP-Routing ist dann erforderlich, wenn Absender und Empfänger in verschiedenen Netzen liegen.

Default Router

Um sicherzustellen, dass IP-Teilnehmer auch Ziele erreichen, die außerhalb des eigenen Netzwerks liegen und die nicht explizit in einer Routingtabelle aufgeführt sind, muss ein Gateway für die Weiterleitung solcher Pakete angegeben werden (Default Router). Der Default Router wird die Daten dann an das übergeordnete Netzwerk weiterleiten.

Sie können IP-Routing über einen Default Router sowohl für das Mainboard als auch für das Application Board aktivieren oder deaktivieren.

Statische Routen

Statische Routen werden benutzt, um Daten den Weg zu einem Netzwerk zu benennen, das nicht über den Default Router erreicht werden kann.

Sie können statische Routen sowohl für das Mainboard als auch für das Application Board anlegen.

8.4.1 Wie Sie den Default Router aktivieren oder deaktivieren

Voraussetzungen

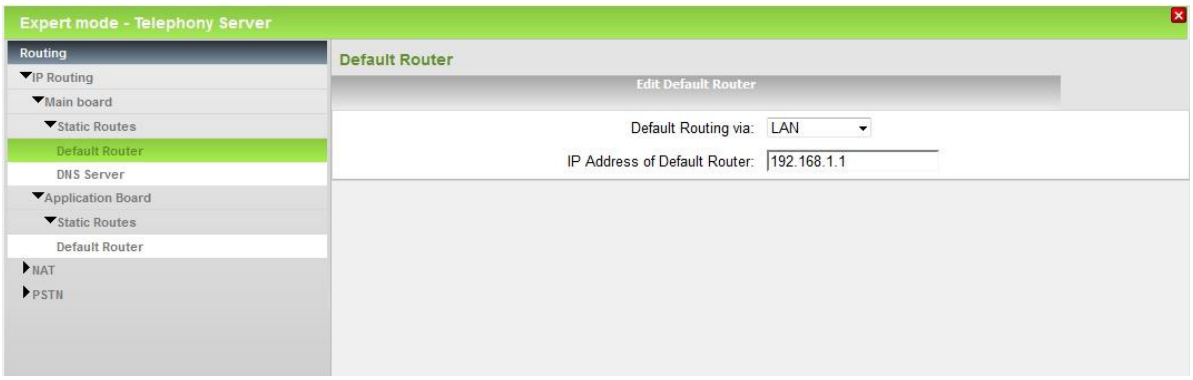
- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Routing**.

3) Navigieren Sie im Menübaum zu **IP-Routing > Mainboard / Application Board > Default Router**. Das Fenster **Default-Router ändern** wird angezeigt.



4) Wenn Sie IP-Routing über einen Default Router aktivieren möchten, wählen Sie in der Auswahlliste **Default-Routing über** den Eintrag **LAN** aus und geben Sie unter **IP-Adresse des Default Routers** die IP-Adresse des Default Routers an, z. B. die IP-Adresse des Internet-Routers: `192.168.1.1`.

5) Wenn Sie IP-Routing über einen Default Router deaktivieren möchten, wählen Sie in der Auswahlliste **Default-Routing über** den Eintrag **Keine Schnittstelle** aus.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

8.4.2 Wie Sie eine statische Route hinzufügen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

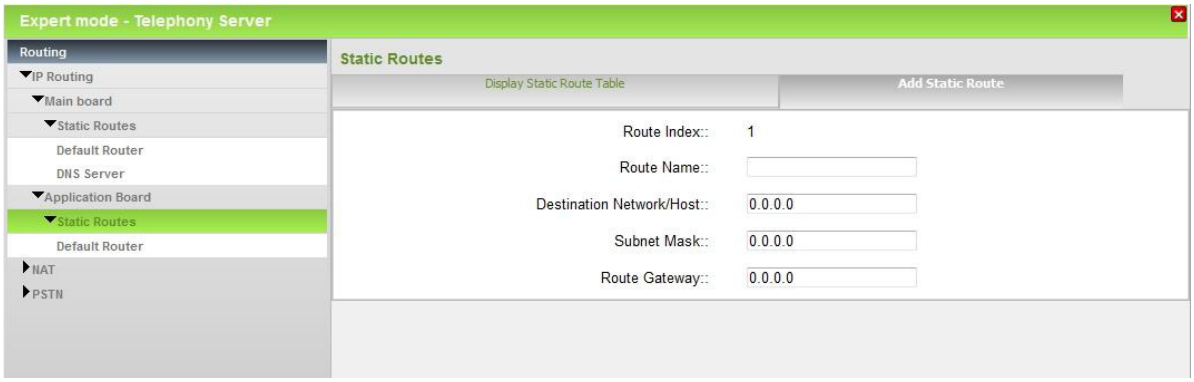
Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Routing**.

3) Navigieren Sie im Menübaum zu **IP-Routing > Mainboard / Application Board > Statische Route**. Das Fenster **Statische Routen** wird angezeigt.

4) Klicken Sie auf die Registerkarte **Statische Route hinzufügen.** Der **Route-Index** zeigt an, welche Route hinzugefügt wird.



5) Im Feld **Route-Name** geben Sie den gewünschten Namen für diese Route an.

6) Geben Sie die IP-Adresse des **Ziel-Netzwerk/Host** ein.

7) Geben Sie die IP-Adresse der **Ziel-Netzmaske** (Subnetzmaske) ein.

8) Geben Sie im Feld **Route-Gateway** die IP-Adresse des Routers ein, über den das gewünschte Zielnetzwerk erreicht werden soll.

9) Wenn Sie eine oder mehrere statische Routen für das Mainboard angelegt haben, können Sie alle statische Routen des Mainboards mit der Schaltfläche **Copy to OCAB** zum Application Board kopieren.

10) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

8.4.3 Wie Sie statische Routen löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Routing**.

3) Navigieren Sie im Menübaum zu **IP-Routing > Mainboard / Application Board > Statische Routen**.

4) Markieren Sie die zu löschende Route.

5) Wechseln Sie auf die Registerkarte **Statische Route löschen**.

6) Klicken Sie auf **Löschen**.

7) Bestätigen sie die Hinweismeldung und klicken Sie anschließend auf **OK**.

8.5 Deployment Service (DLI und DLS)

Mit Hilfe von DLI und DLS können IP-Komponenten zentral administriert und mit Software versorgt werden. Der DLI ist im Kommunikationssystem integriert, der DLS eine eigenständige Applikation, die auf einem externen Server-PC installiert werden muss.

DLI (Deployment Server Integrated)

Der DLI ist eine im Kommunikationssystem integrierte Komponente, die eingeschränkte DLS-Funktionalität zur Verfügung stellt. Mit dem internen DLI lassen sich alle am Kommunikationssystem angeschlossenen IP-Systemtelefone zentral konfigurieren und automatisch mit der aktuellsten Telefon-Software versehen.

Das interne DLI arbeitet mit dem ebenfalls integrierten FTP-Server zusammen, auf dem die aktuellste Telefon-Software gespeichert ist.

Ist dem DHCP-Server die IP-Adresse des DLI bekannt, sendet der DHCP-Server diese Daten an das IP-Systemtelefon (HFA, SIP), sobald es sich im internen Netz anmeldet. Somit kann sich das Telefon die aktuelle Software vom FTP-Server des Kommunikationssystems holen. Im internen DHCP-Server ist standardmäßig der DLI konfiguriert. Soll stattdessen ein externer DLS-Server genutzt werden, muss seine IP-Adresse im internen DHCP-Server konfiguriert werden.

DLS (Deployment Service)

Der DLS ist eine Client/Server-Applikation zur zentralen Administration der IP-Komponenten. Der DLS-Server ist nicht im Kommunikationssystem intergriert und muss separat auf einem Server-PC installiert werden. Der DLS-Client läuft auf den IP-Komponenten. Die Administration erfolgt über einen Web-Browser.

IP-Komponenten sind IP-Systemtelefone, SIP-Telefone, SIP-Clients und IP-Gateways.

> ***INFO:*** Die Eigenschaften und Leistungsmerkmale des DLS sind in der Produktbeschreibung des DLS zu finden und werden nicht in dieser Dokumentation beschrieben.

DLI oder DLS mit externem DHCP-Server

Damit auch bei Nutzung eines externen DHCP-Servers die Software der IP-Systemtelefone (HFA, SIP) automatisch aktualisiert werden kann, haben Sie folgende Alternativen:

- IP-Adresse des DLI oder DLS im externen DHCP-Server konfigurieren
  bei dem externen DHCP-Server müssen die netzwerkspezifischen Daten eingetragen werden und die IP-Adresse des verwendeten Deployment-Servers (DLI oder externer DLS-Servers). Zusätzlich muss auf dem externen DLS-Server die aktuelle Telefon-Software gespeichert sein.

- alle IP-Systemtelefone konfigurieren
  bei jedem IP-Systemtelefon muss als DLS-Adresse die IP-Adresse des verwendeten Deployment-Servers eingetragen werden (IP-Adresse des Kommunikationssystems für den internen DLI oder IP-Adresse des externen DLS-Servers).

Funktionen und Einschränkungen

Funktion	DLI	DLS
zentrale Konfiguration der Parameter der IP-Komponenten Die Parameter der IP-Komponenten sind über anpassbare XML-Templates konfigurierbar.	Ja	Ja
Plug&Play-Inbetriebnahme der IP-Komponenten Über einen DHCP-Server können sich die IP-Komponenten automatisch am System anmelden, z. B bei einem Neuanschluss oder einem Austausch einer IP-Komponente.	Ja	Ja
zentrale & automatische Softwareaktualisierung der IP-Komponenten Die IP-Komponenten werden automatisch beim ersten Anmelden mit der aktuellsten Software-Version versorgt oder wenn eine neue Software-Version zur Verfügung steht. In der IP-Komponente muss die IP-Adresse des DLI/DLS konfiguriert sein.	Ja	Ja auf dem DLS muss die aktuellste Telefon-Software gespeichert sein.
zentrales Inventory-Management der IP-Komponenten Die Daten zu den Hardware-Konfigurationen der IP-Komponenten können zentral abgerufen werden.	Nein	Ja
Unterstützung von IP Mobility (DeskSharing) Telefonie-Daten eines Benutzers werden zentral abgespeichert und können an anderen Telefonen wieder abgerufen werden (z. B. Tastenprogrammierungen, Telefonbucheinträge, Journale).	Ja nicht für SIP-Telefone, nicht im Netzverbund möglich.	Ja nicht für SIP-Telefone, in homogenen Netzen (nur OpenScape Business Systeme) nur bei geschlossener Nummerierung, nicht in inhomogenen Netzen (mit OpenScape 4000 oder OpenScape Voice).
Unterstützung von SPE in Netzen	SPE in Netzen ist derzeit generell nicht möglich, da das SDES-Protokoll nicht implementiert ist. Das gilt unabhängig von DLI/DLS.	SPE in Netzen ist derzeit generell nicht möglich, da das SDES-Protokoll nicht implementiert ist. Das gilt unabhängig von DLI/DLS.
Zentrale Versorgung mehrerer unterschiedlicher Plattformen	Nein	Ja
Freischaltung der 2. LAN-Schnittstelle der IP-Systemtelefone (PC Ethernet Mode). Siehe *Grundeinstellungen > Telefonparameter-Bereitstellung*	Ja	Ja

Deployment und Licensing Client (DLSC)

Um DLS-Funktionen, wie z. B. den Element-Manager, nutzen zu können, muss das Kommunikationssystem dem externen DLS den Zugriff auf die Konfigurationsdaten gewähren. Das Kommunikationssystem wird dann als Deployment und Licensing Client betrieben.

8.5.1 Wie Sie einen externen DLS-Server im internen DHCP-Server konfigurieren

Voraussetzungen

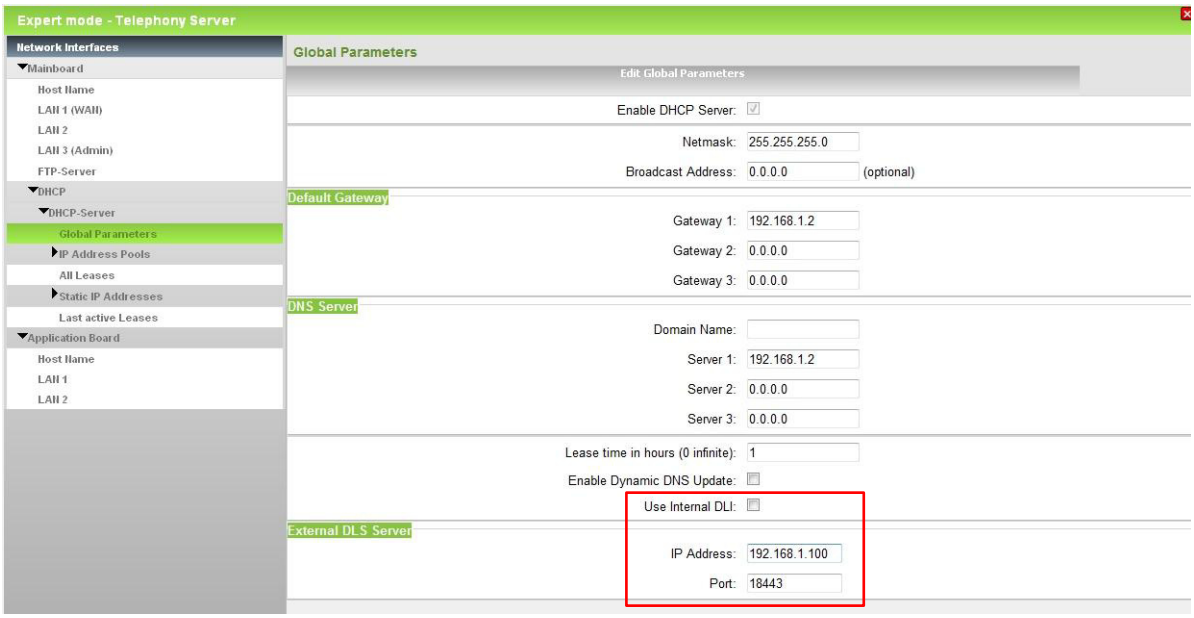
- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Netzwerkschnittstellen**.

3) Navigieren Sie im Menübaum zu **Mainboard > DHCP > DHCP-Server > Globale Einstellungen**. Das Fenster **Globale Parameter ändern** wird angezeigt.



4) Deaktivieren Sie das Kontrollkästchen **Internes DLI verwenden**.

5) Geben Sie im Feld **IP-Adresse** die IP-Adresse ein, unter der der externe DLS-Server zu erreichen ist.

6) Geben Sie im Feld **Port** den Port ein, den der DLS-Server nutzt. Dieser Port muss in der Firewall freigegeben sein.

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

8.5.2 Wie Sie den internen DLI aktivieren

Voraussetzungen

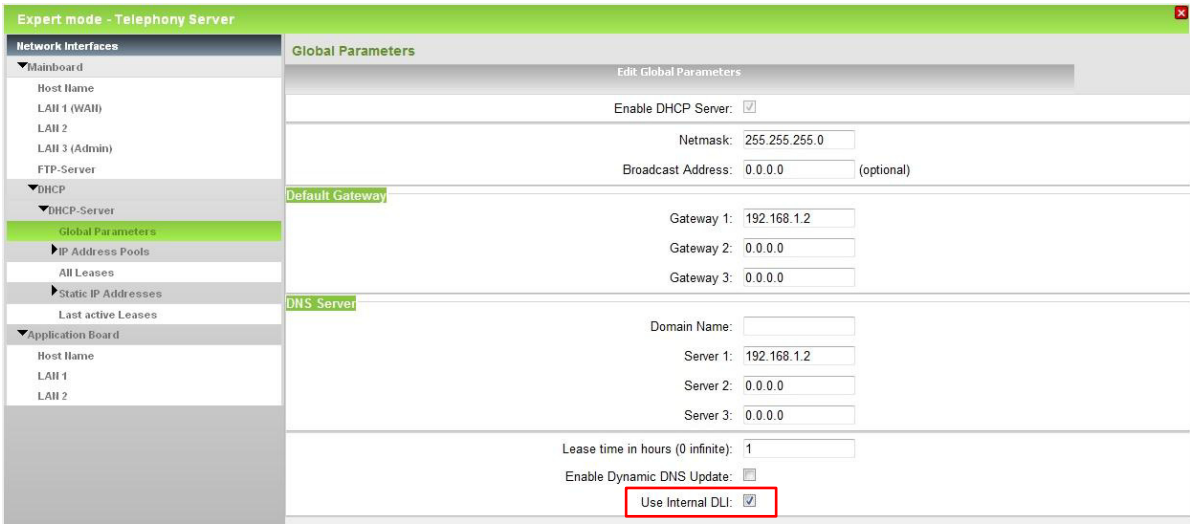
- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Netzwerkschnittstellen**.

3) Navigieren Sie im Menübaum zu **Mainboard > DHCP > DHCP-Server > Globale Einstellungen**. Das Fenster **Globale Parameter ändern** wird angezeigt.



4) Aktivieren Sie das Kontrollkästchen **Internes DLI verwenden**. Das Kontrollkästchen ist standardmäßig aktiviert.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

8.5.3 Wie Sie das Kommunikationssystem als Deployment und Licensing Client konfigurieren

Voraussetzungen

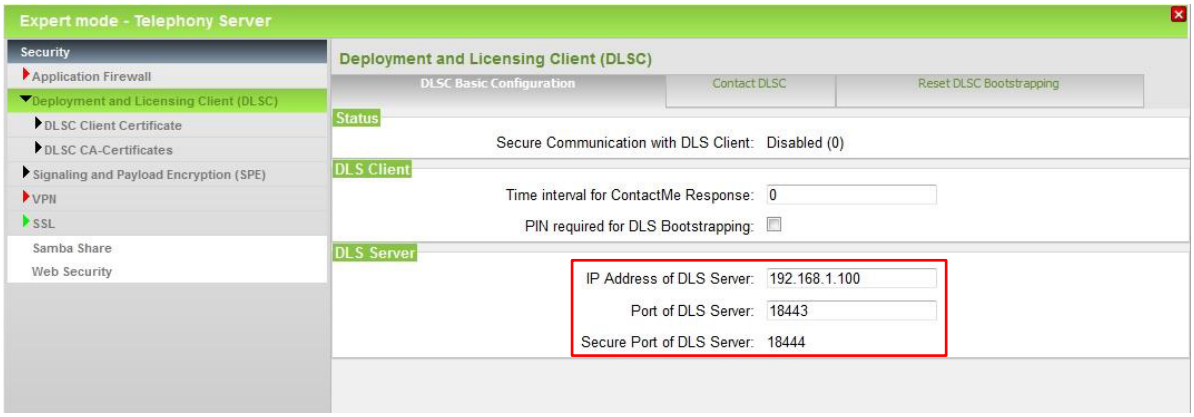
- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.

3) Klicken Sie im Menübaum auf **Deployment- und Licensing-Client (DLSC)**.



4) Geben Sie in der Registerkarte **DLSC Grundeinstellung** im Bereich **DLS-Server** im Feld **IP-Adresse des DLS-Servers** die IP-Adresse ein, unter der der externe DLS-Server zu erreichen ist.

5) Ändern Sie falls nötig unter **Port des DLS-Servers** den Port, den der DLS-Server nutzt. Die beiden angezeigten Ports müssen in der Firewall freigegeben sein.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9 Anbindung an Service-Provider

Das Kommunikationssystem unterstützt die Anbindung an öffentliche Kommunikationsnetze. Die Anbindung an das IP-Netz bietet den Zugang zum Internet und zur Internet-Telefonie, der Amtszugang bietet Zugang zum ISDN-Netz und zum analogen Netz.

Der Zugang zum Internet erfolgt entweder über ein Internet-Modem oder über einen Internet-Router.

Der ISDN-Amtszugang erfolgt bei den Hardware-Plattformen über das Mainboard oder über zusätzlich steckbare Baugruppen. Beim Softswitch ist ein ISDN-Amtszugang nicht möglich.

Der analoge Amtszugang benötigt bei den Hardware-Plattformen eine zusätzlich steckbare Baugruppe. Beim Softswitch ist ein analoger Amtszugang nicht möglich.

9.1 Internet-Zugang

Für den Zugang zum Internet ist eine Breitbandverbindung (DSL-Anschluss oder Kabelanschluss) nötig. Damit ist eine schnelle Datenübertragung im Rahmen der verfügbaren Bandbreite möglich.

Internet-Zugang über DSL-Anschluss

Die Breitbandverbindung zum Internet über DSL (Digital Subscriber Line) erfolgt über die herkömmliche Telefonleitung. Der Internet-Zugang kann parallel zum normalen Telefon genutzt werden. Fax, analoges Telefon oder ISDN stehen auch während der DSL-Verbindung zur Verfügung. Somit lässt sich ein Internet-Zugang realisieren, der wie bei einer Standleitung ständig verfügbar ist (Flatrate).

Für einen Internet-Zugang über DSL benötigen Sie einen Telefonanschluss (analog oder ISDN) und einen Internet-Service-Provider (ISP). Der ISP stellt einen Splitter und ein Internet-Modem (DSL-Modem) bzw. einen Internet-Router mit eingebautem Internet-Modem zur Verfügung. Der Splitter teilt das Signal in die DSL- und Telefonie-Anteile auf und gibt die DSL-Signale an das Internet-Modem weiter.

Das Kommunikationssystem kann direkt an das Internet-Modem oder an den Internet-Router mit integriertem Internet-Modem angeschlossen werden. Im ersten Fall müssen die Zugangsdaten des ISP im Kommunikationssystem eingegeben werden, im zweiten Fall muss dem Kommunikationssystem der Internet-Router bekannt gegeben werden. Die Zugangsdaten des ISP sind im Internet-Router gespeichert.

Um Internet-Telefonie nutzen zu können, benötigen Sie zusätzlich einen Internet-Telefonie-Service-Provider (ITSP, SIP-Provider).

Internet-Zugang über Kabel-Anschluss

Die Breitbandverbindung zum Internet über Kabel erfolgt über den TV-Kabelanschluss. Zusätzlich zur Übertragung der TV-Signale kann der TV-Kabelanschluss für den Zugang zum Internet und zum Telefonieren genutzt werden. Somit ist Surfen und Telefonieren ohne Telefonleitung möglich.

Für einen Internet-Zugang über Kabel benötigen Sie einen Kabelbetreiber, der dieses Leistungsmerkmal anbietet. Er ist zugleich auch Ihr Internet-Service-Provider (ISP). Dieser Kabelbetreiber stellt Ihnen einen Kabelanschluss mit einem Rückkanal und ein Kabelmodem zur Verfügung, das die Daten über das TV-Kabelnetz überträgt. An das Kabelmodem wird der Kabelanschluss und das Kommunikationssystem über Ethernet angeschlossen. Das Herausfiltern der Internetdaten wird im Kabelmodem selbst vorgenommen.

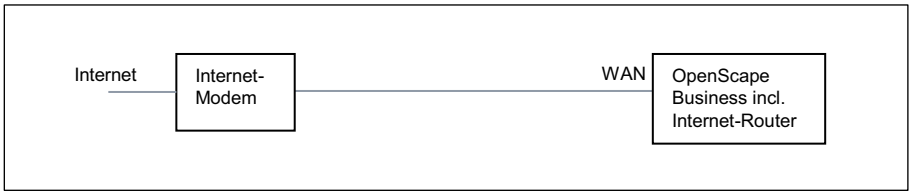
Das Kommunikationssystem kann direkt an das Kabel-Modem angeschlossen werden oder an einen Internet-Router, der wiederum an das Kabelmodem angeschlossen ist. In beiden Fällen muss dem Kommunikationssystem das Kabelmodem oder der Internet-Router bekannt gegeben werden.

Um Internet-Telefonie nutzen zu können, benötigen Sie zusätzlich einen Internet-Telefonie-Service-Provider (ITSP, SIP-Provider).

Konfiguration des Internet-Zugangs

Die Konfiguration des Internet-Zugangs im WBM ist davon abhängig, ob der Internet-Zugang bereits in einem externen Router eingerichtet ist oder ob er über ein Internet-Modem erfolgt und somit im WBM eingerichtet werden muss.

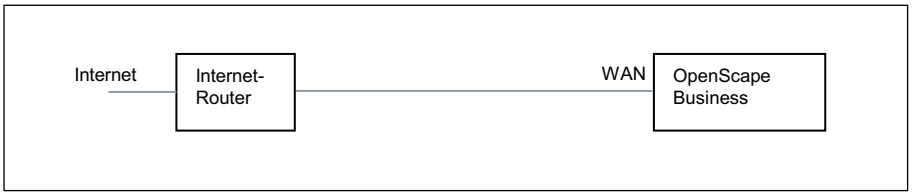
- **Internet-Zugang über ein Internet-Modem** (**DSL am WAN Port direkt**)
  Sie wollen das Kommunikationssystem direkt an einem Internet-Modem (DSL, Kabel, UMTS ...) betreiben. OpenScape Business hat den Internet-Router integriert. Geben Sie die Zugangsdaten des Internet-Service-Providers (ISP) direkt im Kommunikationssystem ein und nutzen den WAN-Anschluss des Kommunikationssystems. Diese Möglichkeit besteht nicht beim Softswitch.

  Sie haben folgende Möglichkeiten:
  - Internet-Zugang über vorkonfigurierten ISP
  - Internet-Zugang über Standard-ISP PPPoE
  - Internet-Zugang über Standard-ISP PPTP

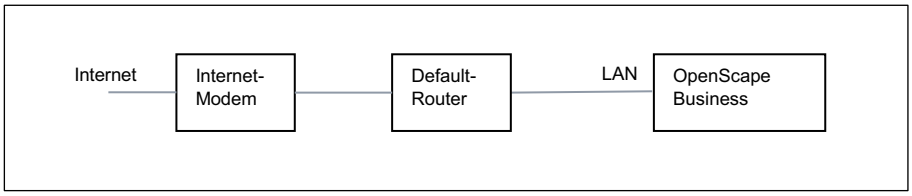
  Ist Ihr ISP nicht unter den vorkonfigurierten ISP, verwenden Sie den Standard-ISP PPPoE oder PPTP.
- **Internet-Zugang über einen externen Internet-Router**
  Sie wollen das Kommunikationssystem an einem externen Internet-Router betreiben. Der Internet-Service-Provider ist bereits im Internet-Router konfiguriert.
  Sie haben folgende Möglichkeiten:

– **Internet-Zugang über externen Internet-Router am WAN-Anschluss** (**TCP/IP am WAN Port über einen externen Router**)



Dazu nutzen Sie den WAN-Anschluss des Kommunikationssystems. OpenScape Business kennt entweder den Internet-Router oder arbeitet als DHCP-Client. Diese Möglichkeit kann verwendet werden, wenn der Internet-Router in einem anderen Netzsegment liegt und einen eigenen DHCP-Server hat.

– **Internet-Zugang über externen Internet-Router am LAN-Anschluss** (**TCP/IP am LAN Port über einen externen Router**)



Dazu nutzen Sie den LAN-Anschluss des Kommunikationssystems. OpenScape Business kennt nur den Default-Router und nicht die dahinterliegende Infrastruktur. Um die Verbindung zum Internet-Router zu aktivieren, muss dem Kommunikationssystem die IP-Adresse des Default-Routers und des DNS-Servers bekannt gegeben werden.

- **Internet-Zugang deaktivieren** (Standardeinstellung)
  Sie wollen das Internet nicht nutzen. Dann lassen Sie den Internet-Zugang deaktiviert.

9.1.1 Internet-Zugang über externen Internet-Router

Mit dem Wizard **Internet-Konfiguration** richten Sie Ihren Internet-Zugang über einen zusätzlichen Internet-Router ein.

Um den Internet-Zugang einzurichten, haben Sie folgende Möglichkeiten:

- **Internet-Zugang über externen Internet-Router am LAN-Anschluss**
  Dazu nutzen Sie den LAN-Anschluss des Kommunikationssystems. Um die Verbindung zum Internet-Router zu aktivieren, muss dem Kommunikationssystem die IP-Adresse des Default-Routers und des DNS-Servers bekannt gegeben werden.
- **Internet-Zugang über externen Internet-Router am WAN-Anschluss**
  Dazu nutzen Sie den WAN-Anschluss des Kommunikationssystems. Diese Möglichkeit kann verwendet werden, wenn der Internet-Router in einem anderen Netzsegment liegt und einen eigenen DHCP-Server hat.

9.1.1.1 Wie Sie den Internet-Zugang über einen externen Internet-Router über den LAN-Anschluss konfigurieren

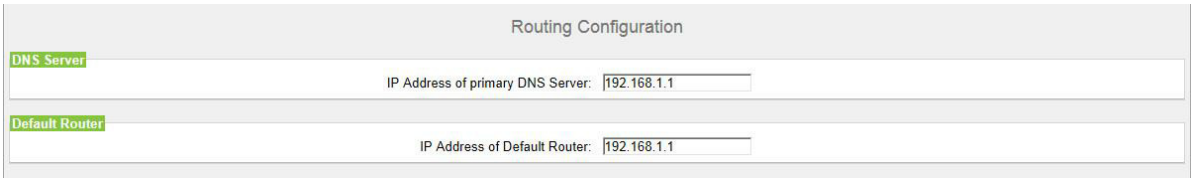
Mit dem Wizard **Internet-Konfiguration** können Sie den Internet-Zugang konfigurieren, wenn das Kommunikationssystem hinter einem zusätzlichen Internet-Router betrieben wird. Kommunikationssystem und der Internet-Router befinden sich im gleichen LAN-Segment. Dazu müssen Sie die IP-Adresse des Internet-Routers und des DNS-Servers eingeben.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.
- Für OpenScape Business X: das Kommunikationssystem ist über die Schnittstelle "LAN" mit dem Kunden-Netz verbunden. Die Verbindung darf nicht über die Schnittstelle "WAN" erfolgen.
- Für OpenScape Business S: der Linux-Server ist über die LAN-Schnittstelle der Netzwerkkarte mit dem Kunden-Netz verbunden.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards > Netzwerk / Internet**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Internet-Konfiguration** zu starten.
4) Deaktivieren Sie das Kontrollkästchen **Kein Internet-Zugang**.
5) Aktivieren Sie das Optionsfeld **TCP/IP am LAN Port über einen externen Router** und klicken Sie auf **OK & Weiter**.



6) Geben Sie im Feld **IP-Adresse des DNS-Servers** die IP-Adresse des lokalen DNS-Servers (z. B. Internet-Router) oder des Internet-DNS-Servers (z. B. für Internet-Telefonie) ein.
7) Geben Sie im Feld **IP-Adresse des Default Routers** die IP-Adresse des externen Internet-Routers ein.
8) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

9.1.1.2 Wie Sie den Internet-Zugang über einen externen Internet-Router über den WAN-Anschluss konfigurieren

Mit dem Wizard **Internet-Konfiguration** können Sie den Internet-Zugang konfigurieren, wenn das Kommunikationssystem hinter einem zusätzlichen Internet-

Router betrieben wird. Kommunikationssystem und Internet-Router müssen sich nicht im gleichen LAN-Segment befinden.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.
- Das Kommunikationssystem muss über die Schnittstelle "WAN" mit dem LAN-Segment des Kundennetzes verbunden sein, indem sich der Internet-Router befindet.
- Sie befinden sich im Fenster **Konfiguration des Internetzugangs**.

Schritt für Schritt

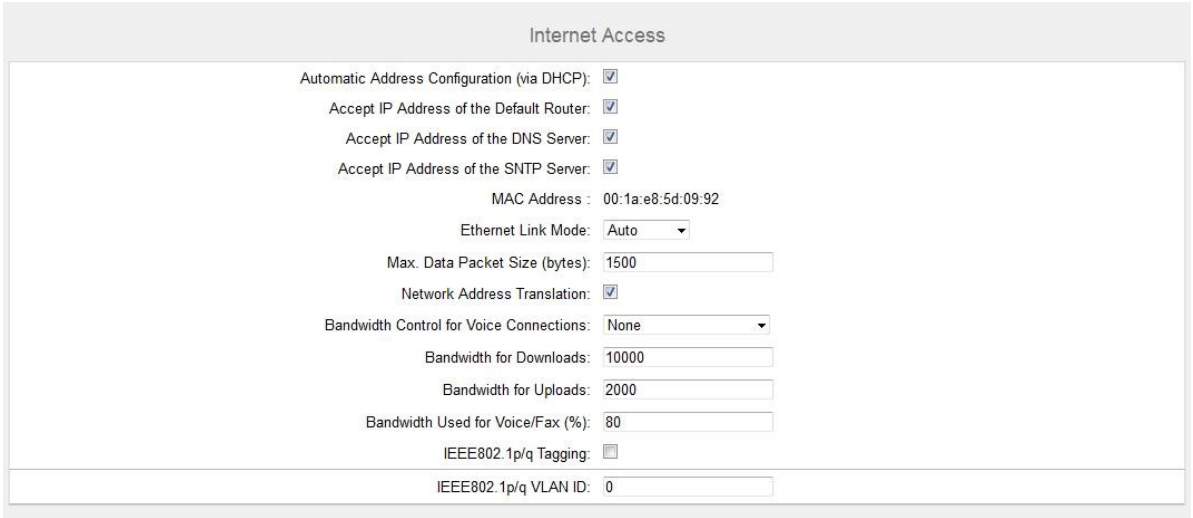
1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Netzwerk / Internet**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Internet-Konfiguration** zu starten.

4) Deaktivieren Sie das Kontrollkästchen **Kein Internet-Zugang**.

5) Aktivieren Sie das Optionsfeld **TCP/IP am WAN Port über einen externen Router** und klicken Sie auf **OK & Weiter**.



6) Wenn für die WAN-Schnittstelle die netzwerkspezifischen Daten von einem bereits aktiven DHCP-Server bezogen werden sollen:

a) Aktivieren Sie das Kontrollkästchen **Automatische Adresskonfiguration (mit DHCP)**.

b) Aktivieren Sie das Kontrollkästchen **IP-Adresse des Default Routers übernehmen**.

c) Aktivieren Sie bei Bedarf das Kontrollkästchen **IP-Adresse des DNS-Servers übernehmen**.

d) Aktivieren Sie bei Bedarf das Kontrollkästchen **IP-Adresse des SNTP-Servers übernehmen**.

7) Wenn der WAN-Schnittstelle eine feste IP-Adresse zugeordnet werden soll:

a) Deaktivieren Sie das Kontrollkästchen **Automatische Adresskonfiguration (mit DHCP)**.

b) Geben Sie die gewünschte **IP-Adresse** und **Netzmaske** der WAN-Schnittstelle ein.

8) Aktivieren Sie das Kontrollkästchen **Netzwerkaddressübersetzung (NAT)**.

9) Wenn Sie zusätzlich Internet-Telefonie nutzen wollen, wählen Sie aus der Aufklappliste **Bandbreitensteuerung für Sprach-Verbindungen** den Eintrag **Nur Upload** oder **Upload und Download** je nach Bedarf aus. Bei einer hohen Download-Bandbreite und zugleich niedrigen Upload-Bandbreite sollte die Bandbreitensteuerung nur für den Upload aktiviert werden, damit nicht unnötig viel Download-Bandbreite für die Sprachübertragung reserviert wird.

10) Geben Sie in den Feldern **Bandbreite Download** und **Bandbreite Upload** die Bandbreite in kbit/s für den Download und Upload ein, die Ihnen Ihr Internet-Service-Provider zur Verfügung stellt.

11) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

9.1.2 Internet-Zugang über Internet-Modem

Mit dem Wizard **Internet-Konfiguration** richten Sie Ihren Internet-Zugang über ein Internet-Modem ein. Dazu wird der WAN-Anschluss des Kommunikationssystems direkt an ein Internet-Modem angeschlossen. Sie können einen im Kommunikationssystem vorkonfigurierten ISP oder einen Standard-ISP-Typ (Typ ist vom ISP zu erfragen) verwenden.

Um den Internet-Zugang einzurichten, haben Sie folgende Möglichkeiten:

- **Internet-Zugang über vorkonfigurierten ISP einrichten**
  Sie nutzen einen im Kommunikationssystem vorkonfigurierten ISP. Dann können Sie aus einer Liste Ihren vorkonfigurierten ISP auswählen.
- **Internet-Zugang über Standard-ISP PPPoE einrichten**
  Sie nutzen den Standard-ISP-Typ **Provider PPPoE**. Erfragen Sie die notwendigen Einstellungen von Ihrem ISP.
- **Internet-Zugang über Standard-ISP PPTP einrichten**
  Sie nutzen den Standard-ISP-Typ **Provider PPTP**. Erfragen Sie die notwendigen Einstellungen von Ihrem ISP.

Verbindungstrennung in Abhängigkeit vom Tarifmodell

Abhängig vom Tarifmodell kann definiert werden, ob die Verbindung zum ISP bei Inaktivität aufrechterhalten werden soll oder nicht.

- Bei dem Tarifmodell Flatrate muss bei Inaktivität keine Trennung der Internet-Verbindung erfolgen. Viele ISP fordern alle 24 Stunden eine Zwangstrennung. Der Zeitpunkt, zu der die Verbindung getrennt werden soll, kann angegeben werden.

- Bei dem Tarifmodell Zeittarif soll die Internet-Verbindung bei Inaktivität getrennt werden. Die Zeitdauer der Inaktivität, nach der die Verbindung getrennt werden soll (z. B. 60 Sekunden) kann angegeben werden. Bei der nächsten Internet-Anforderung wird die Verbindung automatisch wieder aufgebaut. Ist VPN konfiguriert, darf die Verbindung nicht bei Inaktivität getrennt werden - hier sollte das Tarifmodell Flatrate gewählt werden.

  INFO: Programme oder Dienste im Netzwerk können automatisch eine Internet-Verbindung aufbauen und Ihnen dadurch bei einem Zeittarif zusätzliche Verbindungskosten verursachen.

Bandbreite

Der ISP stellt für den Download und den Upload von Daten unterschiedliche Bandbreiten zur Verfügung. Die Bandbreite wird in kbit/s angegeben. Wird zusätzlich Internet-Telefonie genutzt, teilen sich Sprachübertragung und Datenübertragung die Bandbreite. Deshalb ist es sinnvoll, für eine gute Sprachqualität der Sprachübertragung eine ausreichend hohe Bandbreite zu reservieren. Allerdings kann dies bei intensiver Sprachübertragung zu Engpässen bei der Datenübertragung (z. B. langsamere Downloads) führen.

Sie können wählen, ob die Bandbreitensteuerung für Sprachverbindungen nur für den Upload aktiv sein soll oder für Upload und Download zusammen. Bei einer hohen Download-Bandbreite und zugleich niedrigen Upload-Bandbreite sollte die Bandbreitensteuerung nur für den Upload aktiviert werden, damit nicht unnötig viel Download-Bandbreite für die Sprachübertragung reserviert wird.

INFO: Für ein Internet-Gespräch werden ca. 128 kbit/s Bandbreite reserviert.

9.1.2.1 Wie Sie den Internet-Zugang über einen vorkonfigurierten ISP konfigurieren

Mit dem Wizard **Internet-Konfiguration** können Sie Ihren Internet-Zugang über einen im Kommunikationssystem vorkonfigurierten Internet-Service-Provider (ISP) konfigurieren.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.
- Die Internet-Zugangsdaten Ihres ISP liegen Ihnen vor (z. B. Benutzerkennung, Passwort).

Schritt für Schritt

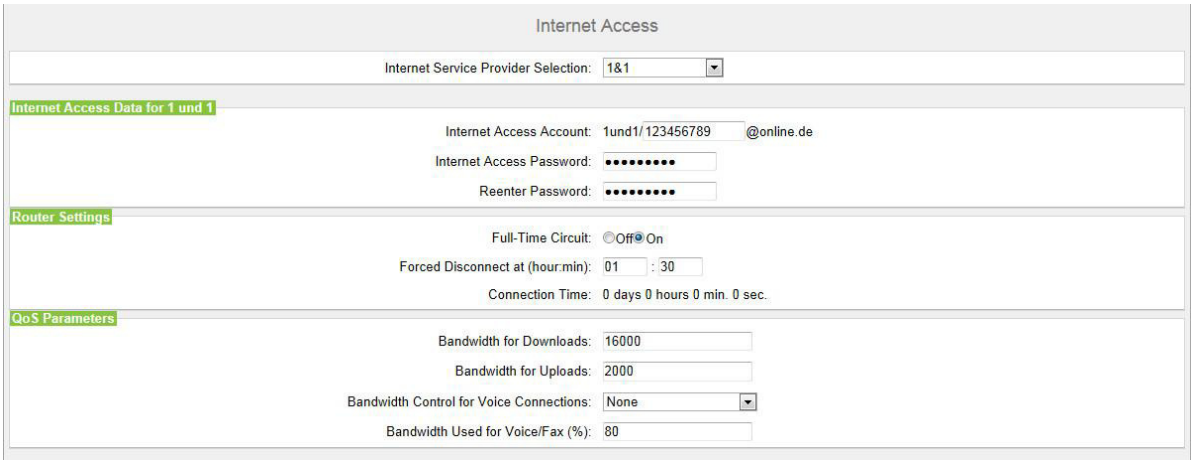
1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Netzwerk / Internet**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Internet-Konfiguration** zu starten.

4) Deaktivieren Sie das Kontrollkästchen **Kein Internet-Zugang**.

5) Aktivieren Sie das Optionsfeld **DSL am WAN Port direkt** und klicken Sie auf **OK & Weiter**.



6) Wählen Sie aus der Aufklappliste **Internet-Service-Provider-Auswahl** Ihren ISP aus.

7) Geben Sie im Bereich **Internet-Zugangsdaten für...** die Zugangsdaten ein, die Sie von ihrem ISP bekommen haben. Die Felder in diesem Bereich sind providerabhängig. Achten Sie bei der Eingabe der Daten auf korrekte Groß- und Kleinschreibung.

8) Wählen Sie im Bereich **Router-Einstellungen** unter **Dauerverbindung** abhängig von Ihrem Tarifmodell eine der beiden folgenden Optionen aus:

- Haben Sie als Tarifmodell eine Flatrate, aktivieren Sie das Optionsfeld **An**. Legen Sie im Feld **Zwangstrennung um (Std:Min)** die Uhrzeit fest, zu der die Internet-Verbindung getrennt werden soll (z. B. 04:59).
- Haben Sie als Tarifmodell einen Zeittarif, aktivieren Sie das Optionsfeld **Aus**. Geben Sie im Feld **Automatisch trennen nach (Sekunden)** die Zeitdauer der Inaktivität an, nach der die Verbindung getrennt werden soll (z. B. 60 Sekunden).

9) Stellen Sie im Bereich **QoS-Parameter** die folgenden Werte ein:

a) Geben Sie in den Feldern **Bandbreite Download** und **Bandbreite Upload** die Bandbreite in kbit/s für den Download bzw. Upload ein, die Ihnen Ihr ISP zur Verfügung stellt.

b) Wenn Sie zusätzlich Internet-Telefonie nutzen wollen, wählen Sie aus der Aufklappliste **Bandbreitensteuerung für Sprach-Verbindungen** den Eintrag **Nur Upload** oder **Upload und Download** je nach Bedarf aus. Geben Sie im Feld **Bandbreite für Sprach-/Fax-Verbindungen (%)** in Prozent an, wieviel Bandbreite für Sprach- und Fax-Verbindungen reserviert werden soll (Standardwert: 80%).

10) Klicken Sie auf **OK & Weiter**. Sie werden zum Fenster **DynDNS-Account einrichten** geführt.

11) Wenn Sie VPN oder den Remote-Zugang nutzen wollen und keine öffentliche statische IP-Adresse haben, müssen Sie einen DynDNS-Account beantragt haben (z. B. bei dyndns.org) und ihn einrichten.

a) Wenn Ihr gewünschter DynDNS-Anbieter in der Aufklappliste **Domainname** enthalten ist, wählen Sie ihn aus der Liste aus (z. B. dyndns.org).

b) Wenn Ihr gewünschter DynDNS-Anbieter nicht in der Aufklappliste **Domainname** enthalten ist, aktivieren Sie das Kontrollkästchen **Benutzerdefinierte Domäne**. Geben Sie im Feld **Domainname** den gewünschten DynDNS-Anbieter ein und in dem Feld **Update-URL** die Update-URL des DynDNS-Anbieters. Der Aufbau dieser URL ist abhängig vom DynDNS-Anbieter. Zusätzlich sind kundenspezifische Parameter (im Beispiel *kursiv* markiert) zu ergänzen.

`http://www.anydns.info/update.php?user=<`*`username`*`>&password=<`*`pass`*`>&host=<`*`domain`*`>&ip=<`*`ipaddr`*`>`

c) Geben Sie **Benutzername** und **Passwort** Ihres DynDNS-Accounts ein.

d) Geben Sie im Feld **Hostname** Ihren vom DynDNS-Anbieter zugeteilten Hostnamen ohne den Domänennamen ein, z. B. myhost. Ihr vollständiger Domänenname lautet dann z. B. myhost.dyndns.org.

e) Testen Sie den DynDNS-Account mit **Verbindung testen**.

f) Klicken Sie nach erfolgreichem Test auf **OK**.

g) Klicken Sie auf **OK & Weiter**.

12) Wenn Sie eine öffentliche statische IP-Adresse haben oder VPN oder den Remote-Zugang nicht nutzen wollen, klicken Sie auf **kein DynDNS**.

13) Klicken Sie auf **Beenden**. Das Kommunikationssystem führt einen Neustart durch.

9.1.2.2 Wie Sie den Internet-Zugang über einen Standard-ISP PPPoE konfigurieren

Mit dem Wizard **Internet-Konfiguration** können Sie Ihren Internet-Zugang über den Standard-Internet-Service-Provider PPPoE konfigurieren.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.
- Folgende Internet-Zugangsdaten Ihres ISP liegen Ihnen vor:

Feld	Beschreibung	Wert vom ISP
IP-Parameter (nur bei fester IP-Adresse)		
Partner-IP-Adresse der PPP-Verbindung	IP-Adresse des Servers Ihres ISP.	
Lokale IP-Adresse der PPP-Verbindung	IP-Adresse, die Ihnen vom ISP für den Internet-Zugang zugeteilt wurde.	
Max. Datenpaketlänge (Byte)	Maximale Paketlänge in Byte, die für das IP-Protokoll gelten soll. Es sind Werte von 576 bis 1500 erlaubt.	
Authentifizierung (über PAP oder CHAP). PAP wird kaum noch verwendet, da die Authentifizierung unverschlüsselt ist.		
PPP-Benutzername	Benutzername für die PPP-Verbindung, der Ihnen vom ISP zugeteilt wurde.	
PAP-Authentifizierungsmode	Authentifizierungsmode für die PPP-Verbindung über PAP: **PAP-Client**, **PAP-Host** oder **nicht benutzt**.	
PAP-Kennwort	Kennwort für Authentifizierung durch PAP, das Ihnen vom ISP zugeteilt wurde.	
CHAP-Authentifizierungsmode	Authentifizierungsmode für die PPP-Verbindung über CHAP: **CHAP-Client**, **CHAP-Host**, **CHAP-Client und -Host** oder **nicht benutzt**.	
CHAP-Kennwort	Kennwort für Authentifizierung durch CHAP, das Ihnen vom ISP zugeteilt wurde.	
QoS-Parameter der Schnittstelle		
Bandbreite Download	Wert der gesamten Bandbreite in kbit/s für den Download vom ISP.	
Bandbreite Upload	Wert der gesamten Bandbreite in kbit/s für den Upload zum ISP.	

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Netzwerk / Internet**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Internet-Konfiguration** zu starten.

4) Deaktivieren Sie das Kontrollkästchen **Kein Internet-Zugang**.

5) Aktivieren Sie das Optionsfeld **DSL am WAN Port direkt** und klicken Sie auf **OK & Weiter**.

6) Wählen Sie aus der Aufklappliste **Internet-Service-Provider-Auswahl** den Standard ISP Typ **Provider-PPPoE** aus.

7) Aktivieren Sie im Bereich **IP-Parameter** das Kontrollkästchen **IP-Parameter** nur, wenn vom ISP eine Anpassung gefordert wird. Geben Sie in diesem Fall in den Feldern **Partner-IP-Adresse der PPP-Verbindung**, **Lokale IP-Adresse der PPP-Verbindung** und **Max. Datenpaketlänge (Byte)** die Werte

ein, die Sie von Ihrem ISP bekommen haben. Wählen Sie aus der Aufklappliste **IP-Address-Aushandlung** den Eintrag **konfigurierte IP-Adresse nutzen** aus.

8) Wählen Sie im Bereich **Router-Einstellungen** unter **Dauerverbindung** abhängig von Ihrem Tarifmodell eine der beiden folgenden Optionen aus:

- Haben Sie als Tarifmodell eine Flatrate, aktivieren Sie das Optionsfeld **An**. Legen Sie im Feld **Zwangstrennung um (Std:Min)** die Uhrzeit fest, zu der die Internet-Verbindung getrennt werden soll (z. B. 04:59).
- Haben Sie als Tarifmodell einen Zeittarif, aktivieren Sie das Optionsfeld **Aus**. Geben Sie im Feld **Automatisch trennen nach (Sekunden)** die Zeitdauer der Inaktivität an, nach der die Verbindung getrennt werden soll (z. B. 60 Sekunden).

9) Die Einstellungen im Bereich **Authentifizierung** hängen davon ab, ob der ISP eine Authentifizierung über PPP fordert oder nicht.

- Authentifizierung wird vom ISP gefordert: Stellen Sie sicher, dass das Kontrollkästchen **PPP-Authentifizierung** aktiviert ist. Geben Sie als PPP-Benutzernamen den Internet-Zugangsnamen des ISP an. Der gebräuchliche Standard ist der Authentifizierungsmode **CHAP-Client**.
- Authentifizierung wird vom ISP nicht gefordert: Stellen Sie sicher, dass das Kontrollkästchen PPP-Authentifizierung deaktiviert ist.

10) Wenn Sie NAT nutzen wollen, aktivieren Sie im Bereich **Adressenübersetzung** das Kontrollkästchen **NAT** (standardmäßig aktiviert).

11) Stellen Sie im Bereich **QoS-Parameter der Schnittstelle** die folgenden Werte ein:

a) Geben Sie in den Feldern **Bandbreite Download** und **Bandbreite Upload** die Bandbreite in kbit/s für den Download bzw. Upload ein, die Ihnen Ihr ISP zur Verfügung stellt.

b) Wenn Sie zusätzlich Internet-Telefonie nutzen wollen, wählen Sie aus der Aufklappliste **Bandbreitensteuerung für Sprach-Verbindungen** den Eintrag **Nur Upload** oder **Upload und Download** je nach Bedarf aus. Geben Sie im Feld **Bandbreite für Sprach-/Fax-Verbindungen (%)** in Prozent an, wieviel Bandbreite für Sprach- und Fax-Verbindungen reserviert werden soll (Standardwert: 80%).

12) Klicken Sie auf **OK & Weiter**. Sie werden zum Fenster **DynDNS-Account einrichten** geführt.

13) Wenn Sie VPN oder den Remote-Zugang nutzen wollen und keine öffentliche statische IP-Adresse haben, müssen Sie einen DynDNS-Account beantragt haben (z. B. bei dyndns.org) und ihn einrichten.

a) Wenn Ihr gewünschter DynDNS-Anbieter in der Aufklappliste **Domainname** enthalten ist, wählen Sie ihn aus der Liste aus (z. B. dyndns.org).

b) Wenn Ihr gewünschter DynDNS-Anbieter nicht in der Aufklappliste **Domainname** enthalten ist, aktivieren Sie das Kontrollkästchen **Benutzerdefinierte Domäne**. Geben Sie im Feld **Domainname** den gewünschten DynDNS-Anbieter ein und in dem Feld **Update-URL** die

Update-URL des DynDNS-Anbieters. Der Aufbau dieser URL ist abhängig vom DynDNS-Anbieter. Zusätzlich sind kundenspezifische Parameter (im Beispiel *kursiv* markiert) zu ergänzen.

```
http://www.anydns.info/
update.php?user=<username>&password=<pass>&host=<doma
in>&ip=<ipaddr>
```

c) Geben Sie **Benutzername** und **Passwort** Ihres DynDNS-Accounts ein.

d) Geben Sie im Feld **Hostname** Ihren vom DynDNS-Anbieter zugeteilten Hostnamen ohne den Domänennamen ein, z. B. myhost. Ihr vollständiger Domänenname lautet dann z. B. myhost.dyndns.org.

e) Testen Sie den DynDNS-Account mit **Verbindung testen**.

f) Klicken Sie nach erfolgreichem Test auf **OK**.

g) Klicken Sie auf **OK & Weiter**.

14) Wenn Sie eine öffentliche statische IP-Adresse haben oder VPN oder den Remote-Zugang nicht nutzen wollen, klicken Sie auf **kein DynDNS**.

15) Klicken Sie auf **Beenden**. Das Kommunikationssystem führt einen Neustart durch.

9.1.2.3 Wie Sie den Internet-Zugang über einen Standard-ISP PPTP konfigurieren

Mit dem Wizard **Internet-Konfiguration** können Sie Ihren Internet-Zugang über den Standard-Internet-Service-Provider PPTP konfigurieren.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.
- Folgende Internet-Zugangsdaten Ihres ISP liegen Ihnen vor:

Feld	Beschreibung	Wert vom ISP
IP-Parameter (nur bei fester IP-Adresse)		
Partner-IP-Adresse der PPP-Verbindung	IP-Adresse des Servers Ihres ISP.	
Lokale IP-Adresse der PPP-Verbindung	IP-Adresse, die Ihnen vom ISP für den Internet-Zugang zugeteilt wurde.	
Max. Datenpaketlänge (Byte)	Maximale Paketlänge in Byte, die für das IP-Protokoll gelten soll. Es sind Werte von 576 bis 1500 erlaubt.	
PPTP-Parameter		
Lokale IP-Adresse der Kontrollverbindung	IP-Adresse, die Ihnen vom ISP für die PPTP-Verbindung zugeteilt wurde. Der voreingestellte Wert lautet 10.0.0.140.	

Feld	Beschreibung	Wert vom ISP
Partner-IP-Adresse der Kontroll-verbindung	IP-Adresse des Servers Ihres ISP für die PPTP-Verbindung. Der voreingestellte Wert lautet 10.0.0.138.	
Partner-Netzmaske für die Kont-rollverbindung	Netzmaske, die Ihnen vom ISP für die PPTP-Verbindung zugeteilt wurde. Der voreingestellte Wert lautet 255.255.255.248.	
Authentifizierung (über PAP oder CHAP). PAP wird kaum noch verwendet, da die Authentifizierung unverschlüsselt ist.		
PPP-Benutzername	Benutzername für die PPP-Verbindung, der Ihnen vom ISP zugeteilt wurde.	
PAP-Authentifizierungsmode	Authentifizierungsmode für die PPP-Verbindung über PAP: **PAP-Client**, **PAP-Host** oder **nicht benutzt**.	
PAP-Kennwort	Kennwort für Authentifizierung durch PAP, das Ihnen vom ISP zugeteilt wurde.	
CHAP-Authentifizierungsmode	Authentifizierungsmode für die PPP-Verbindung über CHAP: **CHAP-Client**, **CHAP-Host**, **CHAP-Client und -Host** oder **nicht benutzt**.	
CHAP-Kennwort	Kennwort für Authentifizierung durch CHAP, das Ihnen vom ISP zugeteilt wurde.	
QoS-Parameter der Schnittstelle		
Bandbreite Download	Wert der gesamten Bandbreite in kbit/s für den Download vom ISP.	
Bandbreite Upload	Wert der gesamten Bandbreite in kbit/s für den Upload zum ISP.	

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Netzwerk / Internet**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Internet-Konfiguration** zu starten.

4) Deaktivieren Sie das Kontrollkästchen **Kein Internet-Zugang**.

5) Aktivieren Sie das Optionsfeld **DSL am WAN Port direkt** und klicken Sie auf **OK & Weiter**.

6) Wählen Sie aus der Aufklappliste **Internet-Service-Provider-Auswahl** den Standard ISP Typ **Provider-PPTP** aus.

7) Aktivieren Sie im Bereich **IP-Parameter** das Kontrollkästchen **IP-Parameter** nur, wenn vom ISP eine Anpassung gefordert wird. Geben Sie in diesem Fall in den Feldern **Partner-IP-Adresse der PPP-Verbindung**, **Lokale IP-Adresse der PPP-Verbindung** und **Max. Datenpaketlänge (Byte)** die Werte ein, die Sie von Ihrem ISP bekommen haben. Wählen Sie aus der Aufklapp-

liste **IP-Address-Aushandlung** den Eintrag **konfigurierte IP-Adresse nutzen** aus.

8) Geben Sie in dem Bereich **PPTP-Parameter** die Werte ein, die Sie von Ihrem ISP bekommen haben.

9) Wenn Sie als Tarifmodell einen Zeittarif haben, aktivieren Sie das Kontrollkästchen **Short-Hold-Modus**. Geben Sie im Feld **Short-Hold-Zeit (s)** die Zeitdauer der Inaktivität an, nach der die Verbindung getrennt werden soll (z. B. 60 Sekunden).

10) Die Einstellungen im Bereich **Authentifizierung** hängen davon ab, ob der ISP eine Authentifizierung über PPP fordert oder nicht.

- Authentifizierung wird vom ISP gefordert: Stellen Sie sicher, dass das Kontrollkästchen **PPP-Authentifizierung** aktiviert ist. Geben Sie als PPP-Benutzernamen den Internet-Zugangsnamen des ISP an. Treffen Sie die PAP- und CHAP-Einstellungen, wie Sie sie von Ihrem ISP zugeteilt bekommen haben.
- Authentifizierung wird vom ISP nicht gefordert: Stellen Sie sicher, dass das Kontrollkästchen PPP-Authentifizierung deaktiviert ist.

11) Wenn Sie NAT nutzen wollen, aktivieren Sie im Bereich **Adressenübersetzung** das Kontrollkästchen **NAT** (standardmäßig aktiviert).

12) Stellen Sie im Bereich **QoS-Parameter der Schnittstelle** die folgenden Werte ein:

a) Geben Sie in den Feldern **Bandbreite Download** und **Bandbreite Upload** die Bandbreite in kbit/s für den Download bzw. Upload ein, die Ihnen Ihr ISP zur Verfügung stellt.

b) Wenn Sie zusätzlich Internet-Telefonie nutzen wollen, wählen Sie aus der Aufklappliste **Bandbreitensteuerung für Sprach-Verbindungen** den Eintrag **Nur Upload** oder **Upload und Download** je nach Bedarf aus. Geben Sie im Feld **Bandbreite für Sprach-/Fax-Verbindungen (%)** in Prozent an, wieviel Bandbreite für Sprach- und Fax-Verbindungen reserviert werden soll (Standardwert: 80%).

13) Klicken Sie auf **OK & Weiter**. Sie werden zum Fenster **DynDNS-Account einrichten** geführt.

14) Wenn Sie VPN oder den Remote-Zugang nutzen wollen und keine öffentliche statische IP-Adresse haben, müssen Sie einen DynDNS-Account beantragt haben (z. B. bei dyndns.org) und ihn einrichten.

a) Wenn Ihr gewünschter DynDNS-Anbieter in der Aufklappliste **Domainname** enthalten ist, wählen Sie ihn aus der Liste aus (z. B. dyndns.org).

b) Wenn Ihr gewünschter DynDNS-Anbieter nicht in der Aufklappliste **Domainname** enthalten ist, aktivieren Sie das Kontrollkästchen **Benutzerdefinierte Domäne**. Geben Sie im Feld **Domainname** den gewünschten DynDNS-Anbieter ein und in dem Feld **Update-URL** die Update-URL des DynDNS-Anbieters. Der Aufbau dieser URL ist

abhängig vom DynDNS-Anbieter. Zusätzlich sind kundenspezifische Parameter (im Beispiel *kursiv* markiert) zu ergänzen.

```
http://www.anydns.info/
update.php?user=<username>&password=<pass>&host=<doma
in>&ip=<ipaddr>
```

c) Geben Sie **Benutzername** und **Passwort** Ihres DynDNS-Accounts ein.

d) Geben Sie im Feld **Hostname** Ihren vom DynDNS-Anbieter zugeteilten Hostnamen ohne den Domänennamen ein, z. B. myhost. Ihr vollständiger Domänenname lautet dann z. B. myhost.dyndns.org.

e) Testen Sie den DynDNS-Account mit **Verbindung testen**.

f) Klicken Sie nach erfolgreichem Test auf **OK**.

g) Klicken Sie auf **OK & Weiter**.

15) Wenn Sie eine öffentliche statische IP-Adresse haben oder VPN oder den Remote-Zugang nicht nutzen wollen, klicken Sie auf **kein DynDNS**.

16) Klicken Sie auf **Beenden**. Das Kommunikationssystem führt einen Neustart durch.

9.1.3 WAN-Schnittstelle

WANs (**W**ide **A**rea **N**etwork) werden benutzt, um verschiedene LANs (**L**ocal **A**rea **N**etwork), aber auch einzelne PC miteinander zu vernetzen. An die WAN-Schnittstelle kann ein Internet-Modem für den Zugang zum Internet angeschlossen werden.

Die WAN-Schnittstelle darf nicht für die Vernetzung von Netzwerk-Knoten und zum Anschluss von IP-Teilnehmern oder IP-Clients benutzt werden.

9.1.4 DynDNS

DynDNS (Dynamic Domain Name Service) ist ein Internet-Dienst, der einer sich dynamisch ändernde IP-Adresse einen festen DNS-Namen zuordnet.

OpenScape Business X stellt den DynDNS Service zur Verfügung, wenn ein Internet-Modem am WAN-Port von OpenScape Business X angeschlossen ist und das Kommunikationssystem als Internet-Router genutzt wird. Ist dies nicht der Fall, wird DynDNS im externen Internet-Router in der Infrastruktur des Kunden eingerichtet.

DNS-Name

Ein Client, der mit einer dynamischen IP-Adresse am Internet angeschlossen ist, kann mit Hilfe von DynDNS immer mit demselben Namen, dem DNS-Namen, angesprochen werden. Dazu ist ein DynDNS-Account bei einem DynDNS-Anbieter (z. B. www.dyndns.org) nötig. Wird dem Kommunikationssystem eine neue IP-Adresse zugewiesen (z. B. vom Internet-Service-Provider), wird diese

IP-Adresse automatisch an den DynDNS-Anbieter gesendet und im DynDNS-Account gespeichert. Das Zeitintervall, in der diese Aktualisierung erfolgt, ist einstellbar. Wird ein DNS-Name angesprochen, wird er über eine Anfrage beim DynDNS-Anbieter in die momentan gültige IP-Adresse aufgelöst. Der komplette DNS-Name (auch Domänenname genannt) setzt sich aus dem frei wählbaren Hostnamen (z. B. myhost) und dem ausgewählten DynDNS-Anbieter (z. B. dyndns.org) zusammen, z. B. myhost.dyndns.org. Nähere Informationen finden Sie z. B. unter der Internet-Adresse:

`http://www.dyndns.org/services/dyndns`

Mit DynDNS ist es auch möglich, ein virtuelles privates Netzwerk (VPN) über einen Internet-Service-Provider aufzubauen, der dynamische IP-Adressen liefert. So können z. B. Teleworker über das Internet auf das interne Netz zugreifen. Weitere Informationen finden Sie unter *Virtual Private Network VPN*.

Mail-Exchanger

Der Mail-Exchange-Eintrag (MX-Record) gibt innerhalb des Domain Name Service (DNS) an, zu welcher IP-Adresse E-Mails für den eingerichteten Domänennamen (z. B. myhost.dyndns.org) zu schicken sind. Hinter der angegebenen IP-Adresse muss sich ein Mail-Server (Mail-Exchanger) befinden. Eine E-Mail-Adresse für diesen Domänennamen könnte z. B. folgendermaßen aussehen: mymail@myhost.dyndns.org.

Mit der Funktion Backup MX werden E-Mails, die nicht an den oben eingetragenen Mail-Exchanger zugestellt werden können (weil dieser z. B. temporär nicht verfügbar ist), zwischengespeichert und zugestellt, sobald der Mail-Exchanger wieder verfügbar ist.

9.1.4.1 Wie Sie den DynDNS-Service konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

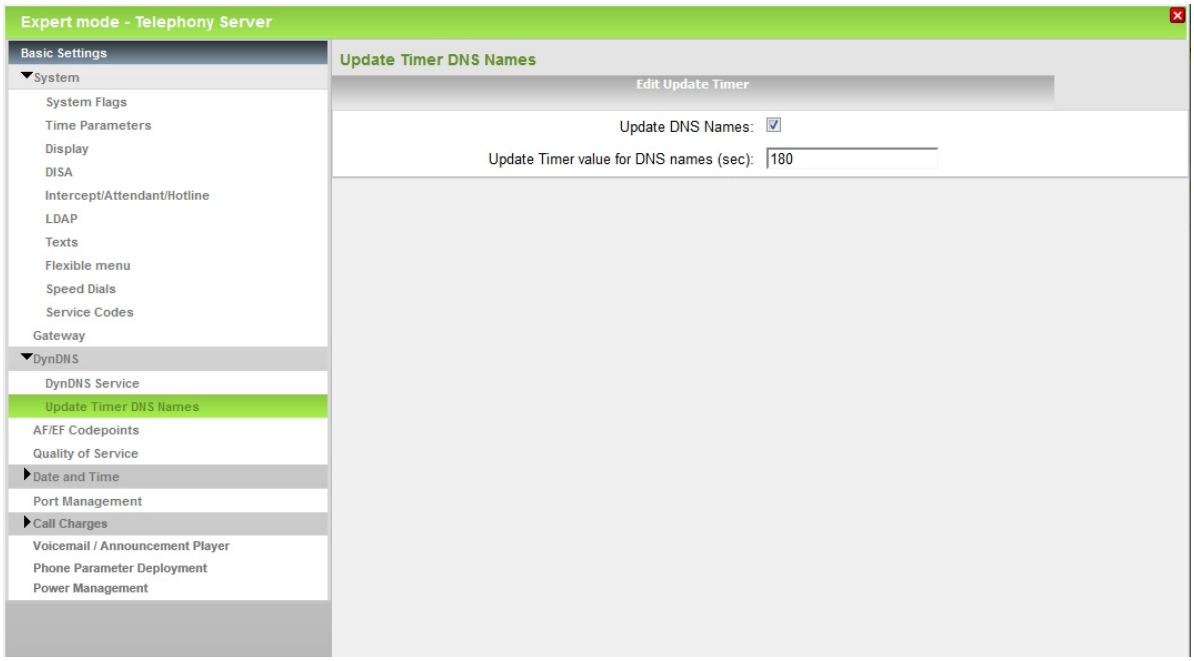
Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **DynDNS**.

4) Klicken Sie auf **Aktualisierungszeit der DNS-Namen**.



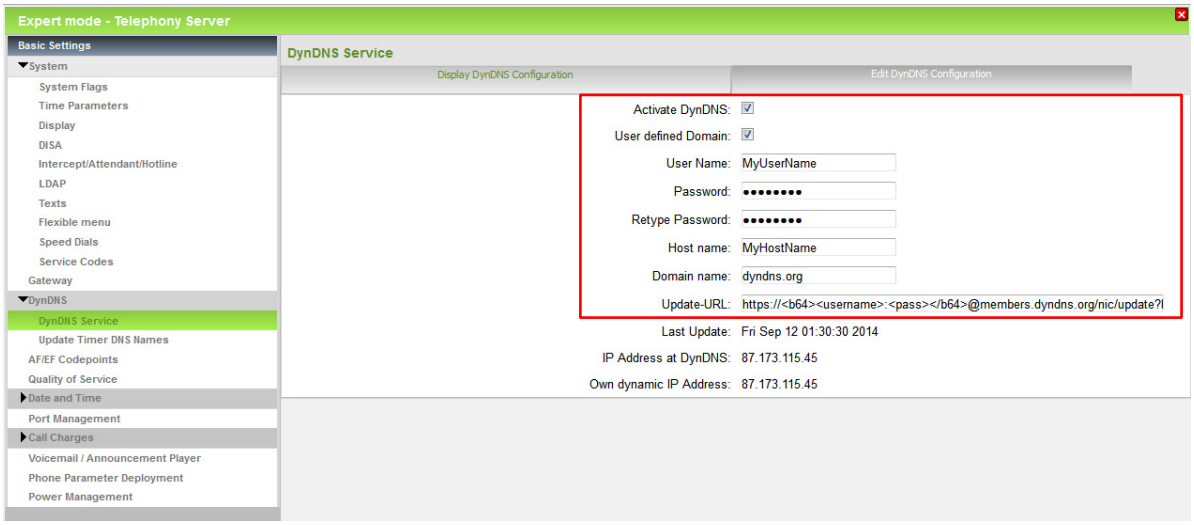
5) Aktivieren Sie das Optionsfeld **DNS-Namen aktualisieren**.

6) Dieser Timer-Wert gilt nur für VPN: Geben Sie im Feld **Timer-Wert für Aktualisierung der DNS-Namen (s)** die Zeit in Sekunden ein, nach der die VPN-Komponente überprüft, ob sich eventuell verwendete DNS-Namen in der VPN-Konfiguration zu neuen IP-Adressen auflösen (VPN mit dynamischen IP-Adressen). In dem Fall wird VPN mit den neuen IP-Adressen rekonfiguriert.

Das Feld ist mit `180` vorbelegt, was einem Aktualisierungsintervall von 3 Minuten entspricht.

7) Klicken Sie im Menübaum auf **DynDNS Service**.

8) Klicken Sie auf die Registerkarte **DynDNS Konfiguration ändern**.



9) Aktivieren Sie das Kontrollkästchen **DynDNS aktivieren**.

10) Wenn Ihr gewünschter DynDNS-Anbieter in der Aufklappliste **Domainname** enthalten ist, wählen Sie ihn aus der Liste aus (z. B. dyndns.org).

11) Wenn Ihr gewünschter DynDNS-Anbieter nicht in der Aufklappliste **Domainname** enthalten ist, aktivieren Sie das Kontrollkästchen **Benutzerdefinierte Domäne**. Geben Sie im Feld **Domainname** den gewünschten DynDNS-Anbieter ein und in dem Feld **Update-URL** die Update-URL des DynDNS-Anbieters. Der Aufbau dieser URL ist abhängig vom DynDNS-Anbieter. Zusätzlich sind kundenspezifische Parameter (im Beispiel *kursiv* markiert) zu ergänzen.

`http://www.anydns.info/update.php?user=`*`<username>`*`&password=`*`<pass>`*`&host=`*`<domain>`*`&ip=`*`<ipaddr>`*

Beispiel einer Update-URL mit Base64 verschlüsselter Authentifizierung:

`https://<b64>`*`<username>`*`:`*`<pass>`*`</b64>@members.dyndns.org/nic/update?hostname=`*`<domain>`*`&myip=`*`<ipaddr>`*`&wildcard=NOCHG&mx=NOCHG&backmx=NOCHG`

<b64>...</b64> für Base64 codierte Parameter

12) Geben Sie im Feld **Benutzername** den Benutzernamen für Ihren DynDNS-Account beim DynDNS-Anbieter ein.

13) Geben Sie in den Feldern **Passwort** und **Passwort wiederholen** das Passwort Ihres DynDNS-Accounts beim DynDNS-Anbieter ein.

14) Geben Sie im Feld **Hostname** Ihren vom DynDNS-Anbieter zugeteilten Hostnamen ohne den Domänennamen ein, z. B. myhost. Ihr vollständiger Domänenname lautet dann z. B. myhost.dyndns.org.

15) Nur sichtbar bei DynDNS-Anbieter, die in der Aufklappliste **Domainname** enthalten sind: Aktivieren Sie das Optionsfeld **Wildcard aktivieren**, wenn auch Anfragen zu einem untergeordneten Domänennamen wie beliebig.myhost.dyndns.org angenommen werden sollen.

16) Nur sichtbar bei DynDNS-Anbieter, die in der Aufklappliste **Domainname** enthalten sind: Aktivieren Sie das Optionsfeld **HTTPS für die Aktualisierung verwenden**, wenn die Aktualisierung der IP-Adresse über eine sichere Verbindung zum DynDNS-Anbieter erfolgen soll.

17) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9.1.4.2 Wie Sie den Mail-Exchanger definieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

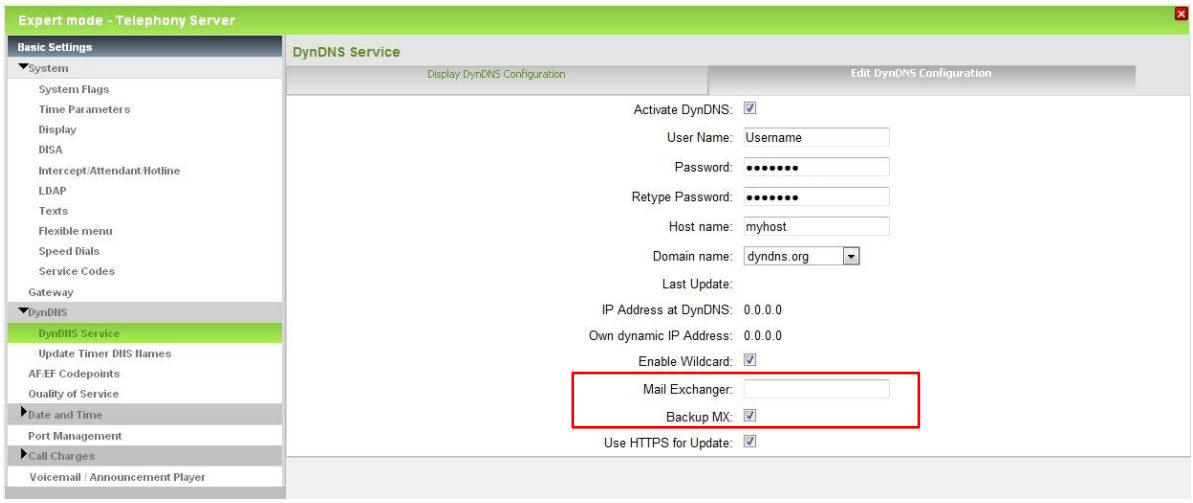
1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **DynDNS**.

4) Klicken Sie auf **DynDNS Service**.

5) Klicken Sie auf die Registerkarte **DynDNS Konfiguration ändern**.



6) Geben Sie im Feld **Mail Exchanger** die IP-Adresse des Mail-Servers (Mail-Exchange-Eintrag bzw. MX-Record) ein.

7) Aktivieren Sie bei Bedarf das Optionsfeld **Backup MX**.

8) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9.2 Amtszugang über ITSP

Um über das Internet zu telefonieren zu können, benötigen Sie einen Zugang zu einem Internet-Telefonie-Service-Provider (ITSP, SIP-Provider). Dazu muss beim ITSP ein Internet-Telefonie-Anschluss und ein Benutzerkonto beantragt werden.

Verbindung zum ITSP

Das Kommunikationssystem nutzt die im Kapitel "Internet-Zugang" beschriebenen Möglichkeiten, den ITSP zu erreichen (OpenScape Business X: über LAN oder WAN / OpenScape Business S: ausschließlich über LAN).

Der ITSP-Zugang basiert auf SIP (Session Initiation Protocol) für die Signalisierung und auf RTP (Realtime Transport Protocol) für Sprache und Daten.

Internet-Telefonie-Service-Provider bieten nicht alle den gleichen Umfang von SIP-Leistungsmerkmalen. Daher sollten nur für das Kommunikationssystem zertifizierte ITSPs genutzt werden. Eine Liste mit den zertifizierten ITSPs sowie den Zertifizierungsprozess finden Sie unter folgendem Link:

`http://wiki.unify.com/wiki/Collaboration_with_VoIP_Providers`

> ***INFO:*** Sonderrufnummern und Notrufnummern, die vom ITSP nicht unterstützt werden, sollten über die Festnetzanschlüsse geführt werden.
>
> Bei Ausfall des ITSP ist über Least Cost Routing (LCR) eine Rückfalllösung über die Festnetzanschlüsse möglich.

ITSP-Benutzerkonto

Das ITSP-Benutzerkonto (SIP User Account) wird beim ITSP beantragt. Der ITSP stellt dafür einen SIP-Registrar-Server zur Verfügung, an dem sich das Kommunikationssystem vorher anmelden muss (providerabhängig).

> ***INFO:*** Eine Registrierung ist nicht notwendig, wenn der ITSP statische IP-Authentifizierung oder VPN-Tunnels verwendet.

Mobile Extension (MEX)

Dieses Leistungsmerkmal wird von einigen Mobilfunkbetreibern in Verbindung mit dem Service MDA (Mobile Direct Access) angeboten. Damit können Mobiltelefone/Smartphones als interne Teilnehmer in ein Kommunikationssystem integriert werden.

Dieses Leistungsmerkmal ist nur mit einem Internet-Telefonie-Durchwahlanschluss nutzbar. Dafür muss bei der Konfiguration des ITSP die vom ITSP zur Verfügung gestellte MEX-Nummer eingetragen werden. Beim ITSP ist die Rufnummer des Mobiltelefons mit der MEX-Nummer verknüpft. Zusätzlich muss das Mobiltelefon/Smartphone im Kommunikationssystem als Mobility-Teilnehmer konfiguriert sein (siehe *Konfiguration von myPortal for Mobile und Mobility Entry*).

Kurzbeschreibung:

- Der Mobilfunkbetreiber bietet ein Flatrate-Angebot für das Mobiltelefon an.
- One Number Service: das Mobiltelefon ist unter einer einzigen Festnetzrufnummer erreichbar, die auch dem Gesprächspartner übermittelt wird.
- Der Anwesenheitsstatus und der Verbindungsstatus von Mobiltelefonen ist genauso wie für interne Teilnehmer sichtbar.
- Jedes Telefonat vom/zum Mobiltelefon wird ausschließlich über OpenScape Business in Kombination mit einem zertifizierten ITSP geführt.
- Die mobile Rufnummer des Mobiltelefons ist nach außen nicht bekannt, d.h. das Mobiltelefon kann nicht direkt angerufen werden. Es kann ebenfalls keine abgehenden, direkten Anrufe tätigen. Alle Rufe führen über OpenScape Business.
- Das Mobiltelefon kann in systeminterne Teams eingebunden werden.
- UC-Anwendungen, wie z. B. myPortal for Desktop und myPortal for Outlook, können wie für interne Teilnehmer genutzt werden. myPortal Smart wird derzeit nicht unterstützt.
- myPortal for Mobile und myPortal to go sind unterwegs nutzbar.
- Eingebundene Mobiltelefone identifizieren sich bei Anruf eines internen Teilnehmers mit ihrem Namen.
- Die Wahlbewertung und das Call-Routing im System bzw. im Netz erfolgt wie für jeden anderen internen Teilnehmer (z.B. erlaubte Rufnummern, verbotene Rufnummern, LCR-Regeln)
- Der ITSP nutzt eine spezielle Anrufsignalisierung von/zur OpenScape Business, die entspr. administriert werden muss.
- Jedes integrierte Mobiltelefon benötigt eine Mobility User Lizenz.
- Um UC-Anwendungen zu nutzen, ist zusätzlich eine UC Client Lizenz erforderlich.

9.2.1 Konfiguration eines ITSP

Es können vordefinierte und neue Internet-Telefonie-Service-Provider (ITSP) konfiguriert werden. Für jeden ITSP können Sie einen oder mehrere Accounts konfigurieren. Es können bis zu 4 ITSP gleichzeitig aktiv sein.

Weiterführende Informationen zu ITSP und deren Leistungsmerkmalen finden Sie hier:

`http://wiki.unify.com/index.php/Collaboration_with_VoIP_Providers#Overview`

INFO: Einrichtebeispiele finden Sie im wiki unter http://wiki.unify.com/images/1/1e/OSBiz_V1_Configuration_for_ITSP.pdf

Zuordnung der ITSP-Rufnummern

- Bei einem **Internet-Telefonie-Teilnehmeranschluss** stellt der ITSP Einzelrufnummern zur Verfügung, z. B. 70005555, 70005556, ... Diese Einzelrufnummern werden anschließend den internen Rufnummern der Teilnehmer manuell zugeordnet.
- Bei einem **Internet-Telefonie-Anlagenanschluss** stellt der ITSP ein Rufnummernband (Rufnummernbereich) zur Verfügung, z. B. (+49) 89 7007-100 bis (+49) 89 7007-147. Die Rufnummern aus dem Rufnummernband werden anschließend den internen Rufnummern der Teilnehmer manuell zugeordnet.

Die beiden Anschlussarten können kombiniert werden.

Alternativ können für beide Anschlussarten die ITSP-Rufnummern bei der Teilnehmer-Konfiguration als Durchwahlrufnummern der Teilnehmer eingetragen werden.

interne Rufnummer	Name	DuWa
100	Andreas Richter	897007100
101	Susanne Mueller	897007101
102	Buddy Miller	897007102
104	Juan Martinez	70005555
105	Emilio Carrara	70005556

Somit ergeben sich die ITSP-Rufnummern aus der eingerichteten Anlagenrufnummer (z. B. Länderkennzahl 49) und den eingetragenen Durchwahlnummern im Langformat. Das hat Vorteile bei der Wahlbewertung und dem Call-Management, auch in einem Netzverbund. So ist der ITSP-Anschluss z. B. durchwahlfähig zu einem anderen Knoten.

Ein weiterer Amtsanschluss über ISDN ist in diesem Fall nur eingeschränkt möglich.

Verwenden von ITSP-Vorlagen

Standard ist es, eine vorkonfigurierte ITSP-Vorlage zu verwenden. Dazu werden in diese Vorlage die eigenen Zugangsdaten und Rufnummern eingetragen und diese anschließend aktiviert.

Im Experten-Modus können Sie auch eine vorkonfigurierte ITSP-Vorlage ändern und als neue Vorlage abspeichern.

Aktualisieren von ITSP-Vorlagen

Die vorkonfigurierten ITSP-Vorlagen werden nach einem Software-Update des Systems automatisch aktualisiert, sofern es in diesem Update neue vorkonfigurierte ITSP-Vorlagen gibt oder aktuellere Standard-Werte für bereits vorhandene vorkonfigurierte Vorlagen.

Ist der ITSP einer Vorlage bereits aktiviert, wird die Aktualisierung nicht automatisch durchgeführt, da bei der Aktualisierung der Standard-Werte wichtige Anpassungen überschrieben werden könnten. Deshalb kann die Aktualisierung bei

Bedarf manuell über den Experten-Modus durchgeführt werden. Anschließend müssen die Standard-Werte wieder an die eigenen Belange angepasst werden.

9.2.1.1 Wie Sie einen vordefinierten ITSP konfigurieren

Mit dem Wizard **Internet-Telefonie** können Sie einen vordefinierten Internet-Telefonie-Service-Provider (ITSP) konfigurieren und aktivieren. Für jeden ITSP können Sie einen oder mehrere Accounts konfigurieren.

Voraussetzungen

- Die Verbindung zum Internet ist betriebsbereit.
- Die Internet-Telefonie-Zugangsdaten Ihres ITSP liegen Ihnen vor (z. B. Benutzerkennung, Passwort, Internet-Telefonie-Rufnummer).
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

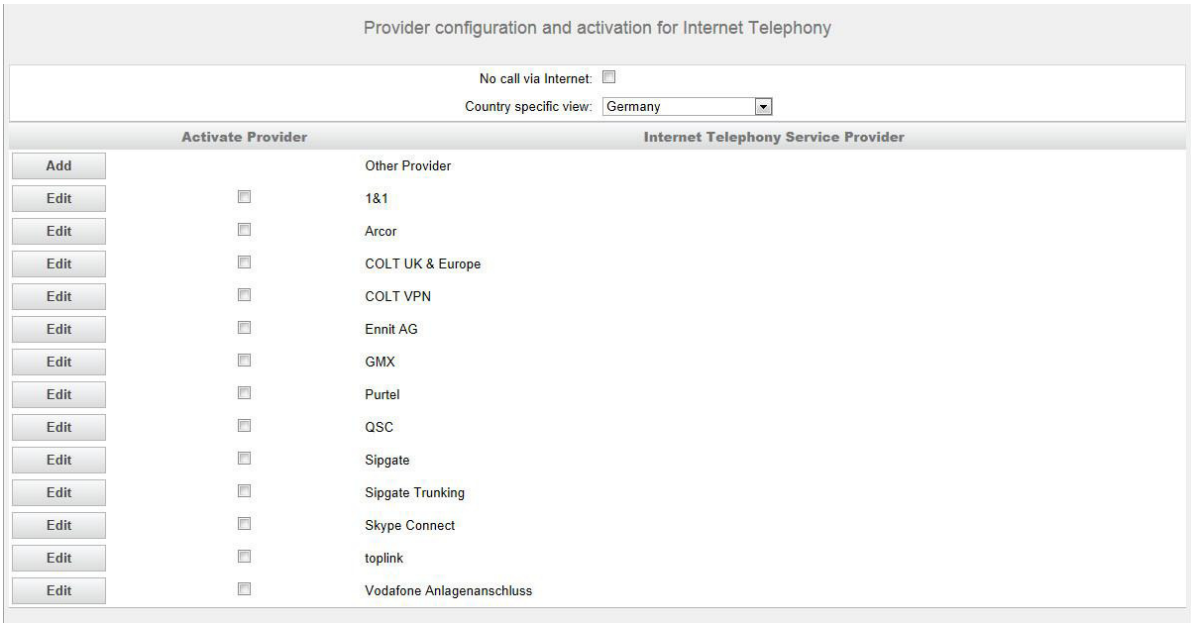
Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Zentrale Telefonie**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Internet-Telefonie** zu starten.

4) Deaktivieren Sie das Kontrollkästchen **Keine Telefonie über Internet**. Es wird Ihnen eine landesabhängige Liste der möglichen ITSP angezeigt. Die Liste enthält die für das gewählte Land vordefinierten ITSP und die eventuell bereits angelegten ITSP.



5) Wenn Sie das voreingestellte Land ändern möchten, wählen Sie aus der Aufklappliste **Länderspezifische Ansicht** das gewünschte Land aus. Es werden die für das gewählte Land möglichen ITSP angezeigt.

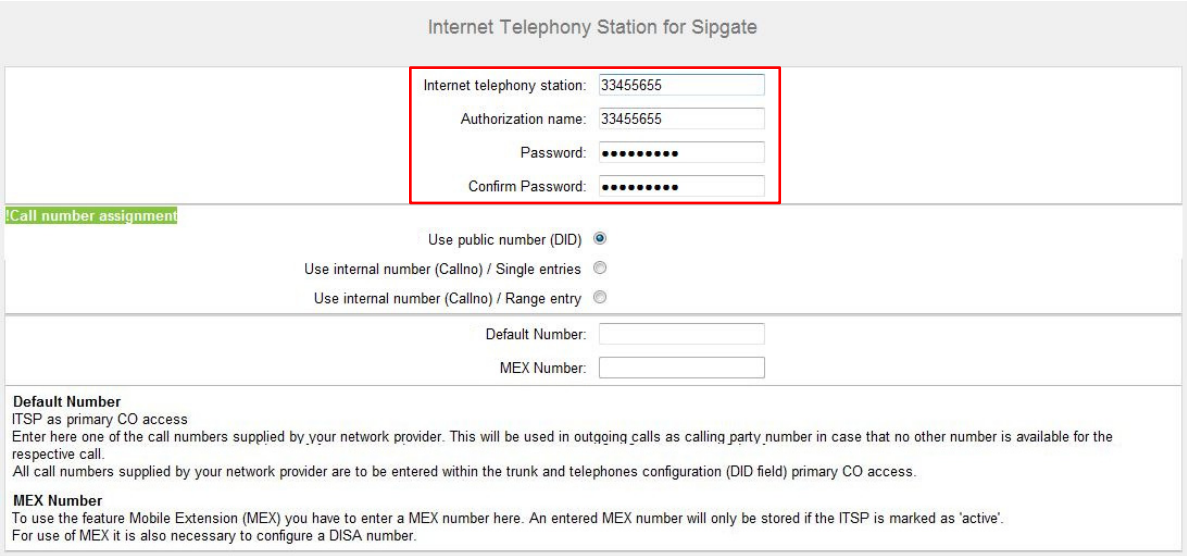
6) Klicken Sie bei Bedarf auf **Status anzeigen**, um abzufragen, welche ITSP bereits aktiviert sind und welche Internet-Telefonie-Teilnehmer unter dem jeweiligen ITSP bereits eingerichtet sind. Maximal können Sie vier ITSP aktivieren. Klicken Sie anschließend auf **OK**.

7) Klicken Sie in der Zeile des gewünschten ITSP auf **Bearbeiten**, um den vordefinierten ITSP zu konfigurieren.

8) Aktivieren Sie das Kontrollkästchen **Provider aktivieren.**

9) Klicken Sie auf **OK & Weiter**.

10) Klicken Sie auf **Hinzufügen**, um Ihre ITSP-Accounts mit den dazugehörigen Internet-Telefonie-Rufnummern zu konfigurieren. Die Felder, die Ihnen anschließend angezeigt werden, sind providerabhängig.



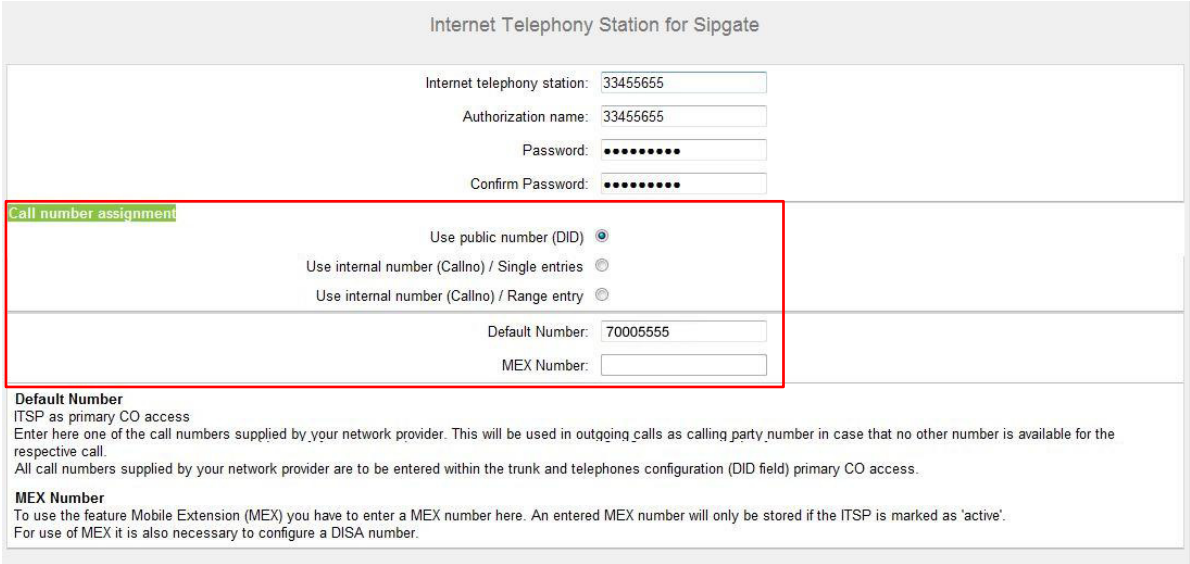
11) Geben im Feld **Internet-Telefonie-Teilnehmer** die Zugangsdaten Ihres Accounts ein. Die Daten haben Sie von Ihrem ITSP erhalten. Je nach ITSP werden hierfür unterschiedliche Bezeichnungen verwendet, wie z. B. SIP-User, SIP-Nutzer, SIP-ID.

12) Geben Sie im Feld **Autorisierungsname** den Autorisierungsnamen ein. Die Daten haben Sie von Ihrem ITSP erhalten. Haben Sie keinen Autorisierungsnamen erhalten, geben Sie die gleichen Daten wie unter **Internet-Telefonie-Teilnehmer** ein.

13) Geben Sie in den Feldern **Neues Kennwort** und **Kennwort wiederholen** das Kennwort an, dass Sie vom ITSP erhalten haben. Je nach ITSP werden hierfür unterschiedliche Bezeichnungen verwendet, wie z. B. SIP-Passwort oder SIP-Kennwort.

14) Zuordnung der Internet-Telefonie-Rufnummern - Möglichkeit 1:

Öffentliche Rufnummer (DuWa): die Internet-Telefonie-Rufnummern Ihres Internet-Telefonie-Teilnehmeranschlusses oder Internet-Telefonie-Anlagenanschlusses werden nicht hier bei der ITSP-Konfiguration, sondern bei der Teilnehmer-Konfiguration in den Feldern **DuWa** eingetragen.



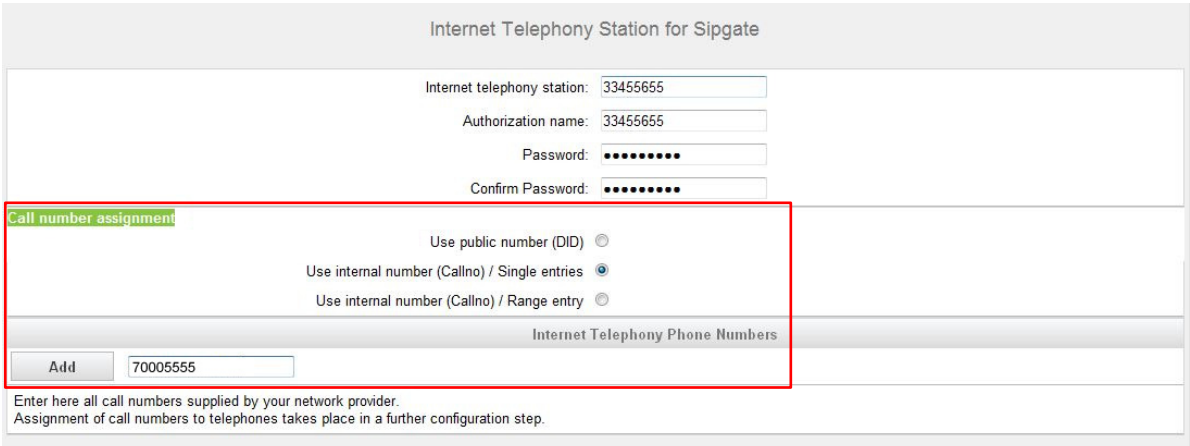
a) Wählen Sie im Bereich **Rufnummer assignment** das Optionsfeld **Öffentliche Rufnummer (DuWa)** aus.

b) Geben Sie unter **Standard-Rufnummer** die Rufnummer ein, die bei gehenden Anrufen für Teilnehmer verwendet werden soll, die keine eigene Rufnummer haben.

c) Falls Ihr ITSP das Leistungsmerkmal "Mobile Extension (MEX)" unterstützt, tragen Sie unter **MEX-Nummer** die vom ITSP zur Verfügung gestellte MEX-Nummer ein (8-stellig, nur Ziffern).

15) Zuordnung der Internet-Telefonie-Rufnummern - Möglichkeit 2:

Interne Nummer (Rufnr.) verwenden / Einzeleinträge: Sie haben einen Internet-Telefonie-Teilnehmeranschluss und als Internet-Telefonie-Rufnummern Einzelrufnummern erhalten (z. B. 70005555, 70005556,...). Diese Einzelrufnummern ordnen Sie anschließend den internen Rufnummern der Teilnehmer zu.



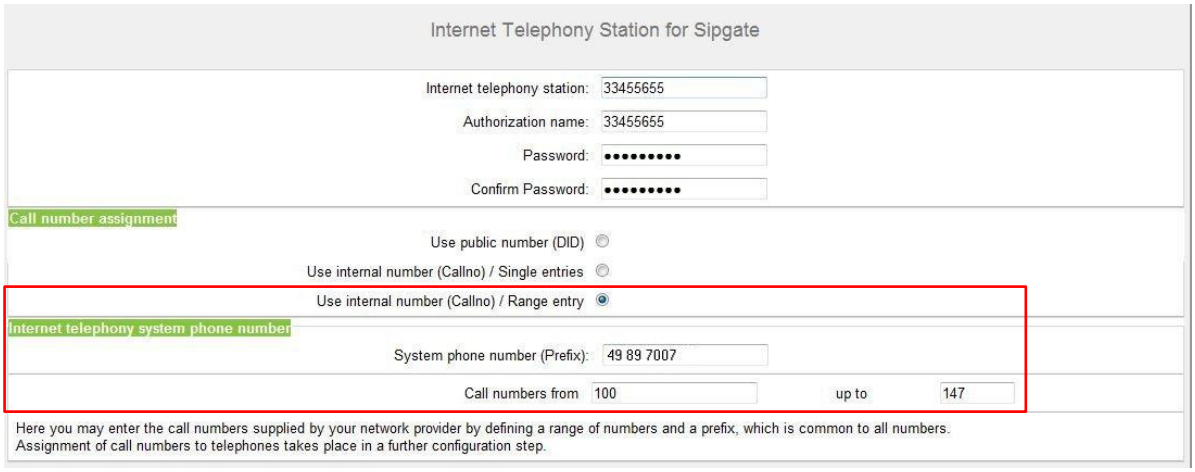
a) Wählen Sie im Bereich **Rufnummer assignment** das Optionsfeld **Interne Nummer (Rufnr.) verwenden / Einzeleinträge** aus.

b) Geben Sie im Bereich **Internet-Telefonie-Teilnehmerrufnummern** im Feld neben der Schaltfläche **Hinzufügen** eine der vom ITSP mitgeteilten Internet-Telefonie-Rufnummern ein und klicken Sie auf **Hinzufügen**.

c) Wenn Sie dem Account weitere Internet-Telefonie-Rufnummern zuordnen wollen, wiederholen Sie Schritt b).

16) Zuordnung der Internet-Telefonie-Rufnummern - Möglichkeit 3:

Interne Nummer (Rufnr.) verwenden / Bereichseintrag: Sie haben einen Internet-Telefonie-Anlagenanschluss und als Internet-Telefonie-Rufnummern ein Rufnummernband erhalten, z. B. (+49) 89 7007-100 bis (+49) 89 7007-147. Die Rufnummern aus dem Rufnummernband ordnen Sie anschließend den internen Rufnummern der Teilnehmer zu.



a) Wählen Sie im Bereich **Rufnummer assignment** das Optionsfeld **Interne Nummer (Rufnr.) verwenden / Bereichseintrag** aus.

b) Geben Sie unter **Anlagenrufnummer (Präfix)** die Anlagenrufnummer ein.

c) Geben Sie in den Feldern **Durchwahlband von** und **bis** das gewünschte Durchwahlband für den Internet-Telefonie-Teilnehmer ein. Standardmäßig ist 100 - 147 eingetragen.

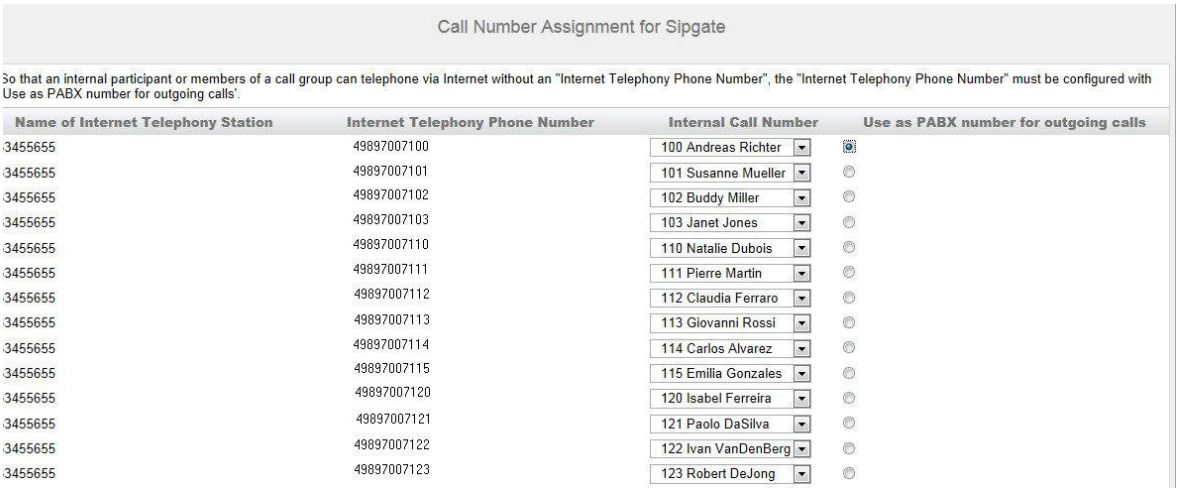
17) Klicken Sie auf **OK & Weiter**.

18) Wenn Sie weitere Accounts einrichten möchten, wiederholen Sie die Schritte 10 bis 17.

19) Klicken Sie auf **OK & Weiter**. Sie sehen eine Übersicht, welche Internet-Telefonie-Rufnummern welchen Accounts zugeordnet sind.

20) Ordnen Sie allen Internet-Telefonie-Rufnummern jeweils einer internen Rufnummer eines Teilnehmers zu.

Dieser Schritt entfällt, wenn Sie für die Zuordnung der Internet-Telefonie-Rufnummern die Möglichkeit 1 gewählt haben. Die Zuordnung treffen Sie in diesem Fall bei der Teilnehmer-Konfiguration im Feld **DuWa**.



Call Number Assignment for Sipgate

So that an internal participant or members of a call group can telephone via Internet without an "Internet Telephony Phone Number", the "Internet Telephony Phone Number" must be configured with Use as PABX number for outgoing calls'.

Name of Internet Telephony Station	Internet Telephony Phone Number	Internal Call Number	Use as PABX number for outgoing calls
3455655	49897007100	100 Andreas Richter	◉
3455655	49897007101	101 Susanne Mueller	○
3455655	49897007102	102 Buddy Miller	○
3455655	49897007103	103 Janet Jones	○
3455655	49897007110	110 Natalie Dubois	○
3455655	49897007111	111 Pierre Martin	○
3455655	49897007112	112 Claudia Ferraro	○
3455655	49897007113	113 Giovanni Rossi	○
3455655	49897007114	114 Carlos Alvarez	○
3455655	49897007115	115 Emilia Gonzales	○
3455655	49897007120	120 Isabel Ferreira	○
3455655	49897007121	121 Paolo DaSilva	○
3455655	49897007122	122 Ivan VanDenBerg	○
3455655	49897007123	123 Robert DeJong	○

a) Wählen Sie in der entsprechenden Zeile aus der Aufklappliste **interne Rufnummer** eine interne Rufnummer aus.

b) Sollen Teilnehmer ohne Internet-Telefonie-Rufnummer oder Mitglieder einer Rufgruppe externe Telefonate über das Internet führen dürfen, muss das Optionsfeld **Als gehende Anlagenrufnummer verwenden** aktiviert sein. Das Optionsfeld kann ausschließlich bei einer einzigen Internet-Telefonie-Rufnummer aktiviert sein.

21) Klicken Sie auf **OK & Weiter**. Hier sehen Sie nochmals die Übersicht der möglichen ITSP. Aktivierte ITSP sind in der Spalte **Provider aktivieren** mit einem Häkchen markiert. Mit **Restart ITSP** können Sie sich bei Verbindungsproblemen bei bereits aktivierten ITSP neu registrieren.

22) Klicken Sie auf **OK & Weiter**.

23) Geben Sie im Feld **Upstream bis zu (Kbit/s)** den Wert der Upload-Geschwindigkeit Ihrer Internet-Verbindung ein. Nicht zu verwechseln mit der Download-Geschwindigkeit!

INFO: Im Feld **Anzahl simultaner Internet-Telefongespräche** wird Ihnen die Anzahl der gleichzeitig zu führenden Internet-Telefongespräche angezeigt. Wenn sich auf Grund der Netzauslastung die Gesprächsqualität verschlechtert, müssen Sie die Anzahl reduzieren.

---

24) Klicken Sie auf **OK & Weiter**.

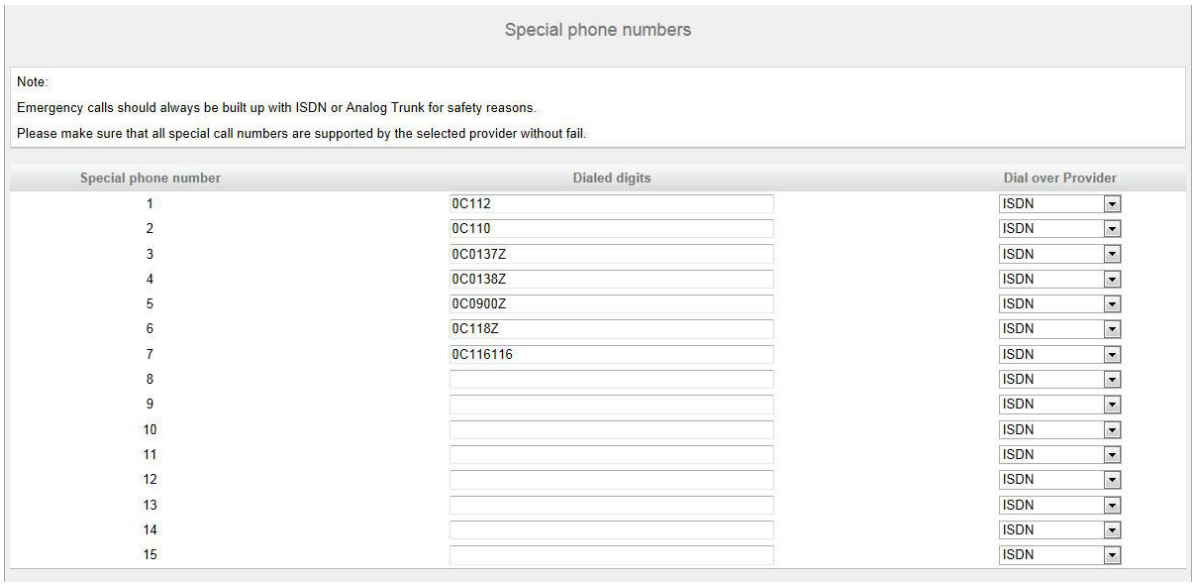
25) Falls Sie bei der Einrichtung Ihres Internet-Zugangs die Dauerverbindung noch nicht aktiviert haben, können Sie das hier nachholen. Ohne Dauerverbindung können Sie keine Anrufe über das Internet empfangen. Ist die Dauerverbindung bereits eingerichtet, erscheinen die unter a) bis c) beschriebenen Felder nicht.

a) Aktivieren Sie unter **Dauerverbindung** das Optionsfeld **An**.

b) Legen Sie im Feld **Zwangstrennung um (Std:Min)** die Uhrzeit fest, zu der die Internet-Verbindung getrennt werden soll (z. B. 04:59).

c) Klicken Sie auf **OK & Weiter**.

26) Tragen Sie in der Spalte **Gewählte Ziffern** die gewünschten Sonderrufnummern ein.



Folgende Rufnummerneinträge sind gültig:

0 bis 9: erlaubte Ziffern

-: Feldtrennzeichen

X: beliebige Ziffer zwischen 0 bis 9

N: beliebige Ziffer zwischen 2 bis 9

Z: eine oder mehrere Ziffern folgen bis Wahlende

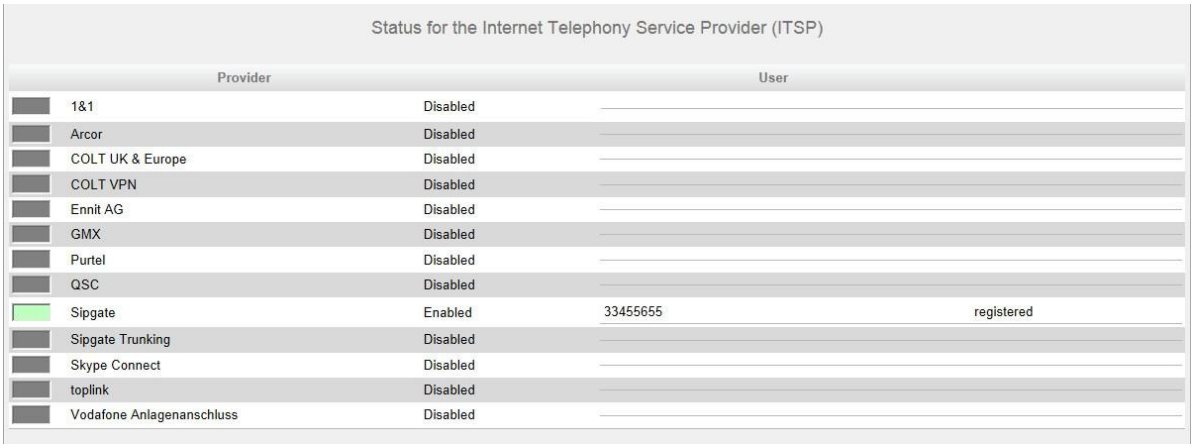
C: simulierter Wählton (kann max. 3 mal eingetragen werden)

27) Wählen Sie in der Spalte **Wählen über Provider** aus, ob die Sonderrufnummer über ISDN oder über einen ITSP gewählt werden soll. Es werden nur aktive ITSP angezeigt.

INFO: Stellen Sie sicher, dass Notrufnummern immer gewählt werden können. Falls Notrufnummern über einen Internet-Telefonie-Service-Provider gewählt werden sollen, muss der ITSP dies unterstützen.

---

28) Klicken Sie auf **OK & Weiter**. Es wird Ihnen der Status der ITSP angezeigt.



29) Klicken Sie auf **Weiter** und anschließend auf **Beenden**. Bitte durchlaufen Sie anschließend den Wizard **Amtsleitung ISDN / Analog / ITSP**, um die Priorisierung für die Amtsholung einzustellen (z. B. Amtsholung zuerst über ITSP und dann über ISDN).

9.2.1.2 Wie Sie einen neuen ITSP hinzufügen

Mit dem Wizard **Internet-Telefonie** können Sie einen neuen Internet-Telefonie-Service-Provider (ITSP) konfigurieren und aktivieren. Für jeden ITSP können Sie einen oder mehrere Accounts konfigurieren.

Voraussetzungen

- Die Verbindung zum Internet ist betriebsbereit.
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.
- Folgende Internet-Zugangsdaten Ihres ITSP liegen Ihnen vor:

Feld	Beschreibung	Wert vom ISP
Gateway Domain Name	Gateway-Domänennamen des ITSP. Meist identisch zum Hostnamen (z. B. sip-voice.de)	
Provider-Registrar		
Provider Registrar verwenden	Wird vom ITSP vorgegeben und ist in der Regel immer gesetzt (nicht nötig bei ITSP, die eine statische P-Authentifizierung verwenden).	
IP-Adresse/Host-Name	Hostname oder IP-Adresse des Registrar-Servers (z. B. sip-voice.de).	
Port	Portnummer des Registrar-Servers (z. B. 5060).	

Feld	Beschreibung	Wert vom ISP
Reregistration-Intervall am Provider (s)	Intervall (in Sekunden), in dem die Registrierung am ITSP wiederholt wird. Der Wert des Intervalls darf nicht 0 sein und sollte nicht zu hoch gesetzt sein, da mit der wiederholten Registrierung am ITSP auch ein Verbindungsausfall erkannt wird und ggf. ein Ersatzweg (über ISDN oder einen alternativen Provider) belegt werden kann. Standardwert: 120 Sekunden.	
Provider-Proxy		
IP-Adresse/Host-Name	Hostname oder IP-Adresse des Proxy-Servers (z. B. sip-voice.de). Ist üblicherweise identisch zum Provider-Registrar-Eintrag.	
Port	Portnummer des Proxy-Servers (z. B. 5060). Ist üblicherweise identisch zur Provider-Registrar-Portnummer.	
Provider-Outbound-Proxy		
Provider Outbound-Proxy verwenden	Wird nur gesetzt, wenn der ITSP einen Outbound-Proxy verwendet.	
IP-Adresse/Host-Name	Hostname oder IP-Adresse des Outbound-Proxy	
Port	Portnummer des Outbound-Proxy	
Provider-Inbound-Proxy		
Provider Inbound-Proxy verwenden	Wird nur gesetzt, wenn der ITSP einen zweiten Proxy verwendet.	
IP-Adresse/Host-Name	Hostname oder IP-Adresse des zweiten Proxy	
Port	Portnummer des zweiten Proxy	
Provider-STUN		
STUN verwenden	Wird nur gesetzt, wenn STUN -Funktionalität benötigt wird. Aktiviert auch den globalen STUN-Modus.	
IP-Adresse/Host-Name	STUN-IP-Adresse, wenn der ITSP einen STUN-Server verwendet.	
Port	STUN-Port-Nummer, wenn der ITSP einen STUN-Server verwendet.	

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards > Zentrale Telefonie**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Internet-Telefonie** zu starten.

4) Deaktivieren Sie das Kontrollkästchen **Keine Telefonie über Internet**. Es wird Ihnen eine landesabhängige Liste der möglichen ITSP angezeigt. Die Liste enthält die für das gewählte Land vordefinierten ITSP und die eventuell bereits angelegten ITSP.

5) Klicken Sie bei Bedarf auf **Status anzeigen**, um abzufragen, welche ITSP bereits aktiviert sind und welche Internet-Telefonie-Teilnehmer unter dem jeweiligen ITSP bereits eingerichtet sind. Maximal können Sie vier ITSP aktivieren. Klicken Sie anschließend auf **OK**.

6) Klicken Sie auf **Hinzufügen**, um einen neuen ITSP einzurichten. Es öffnet sich das Konfigurationsfenster für den neuen ITSP.

7) Vergeben Sie im Feld **Provider-Name** einen Namen Ihrer Wahl für den ITSP.

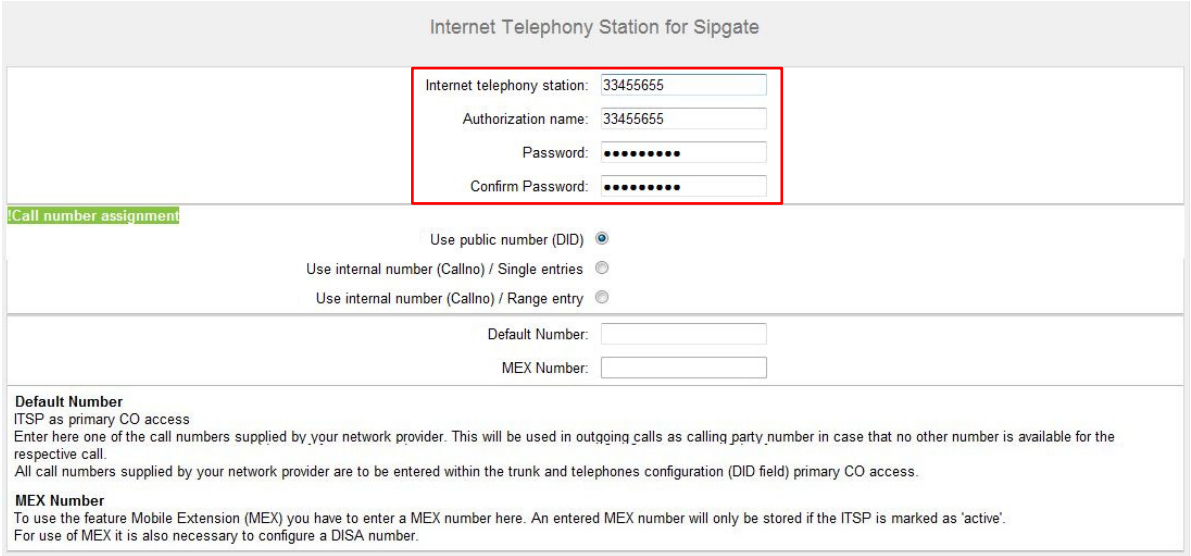
8) Aktivieren Sie das Kontrollkästchen **Provider aktivieren**.

9) Geben Sie in den restlichen Bereichen die Werte ein, die Sie von Ihrem ITSP bekommen haben (siehe Tabelle unter den Voraussetzungen).

> ***INFO:*** Die Werte unter den "erweiterten SIP-Provider Daten" dürfen nur von geschultem Fachpersonal in Zusammenarbeit mit der Entwicklung geändert werden!

10) Klicken Sie auf **OK & Weiter**.

11) Klicken Sie auf **Hinzufügen**, um Ihre ITSP-Accounts mit den dazugehörigen Internet-Telefonie-Rufnummern zu konfigurieren. Die Felder, die Ihnen anschließend angezeigt werden, sind providerabhängig.



12) Geben im Feld **Internet-Telefonie-Teilnehmer** die Zugangsdaten Ihres Accounts ein. Die Daten haben Sie von Ihrem ITSP erhalten. Je nach ITSP werden hierfür unterschiedliche Bezeichnungen verwendet, wie z. B. SIP-User, SIP-Nutzer, SIP-ID.

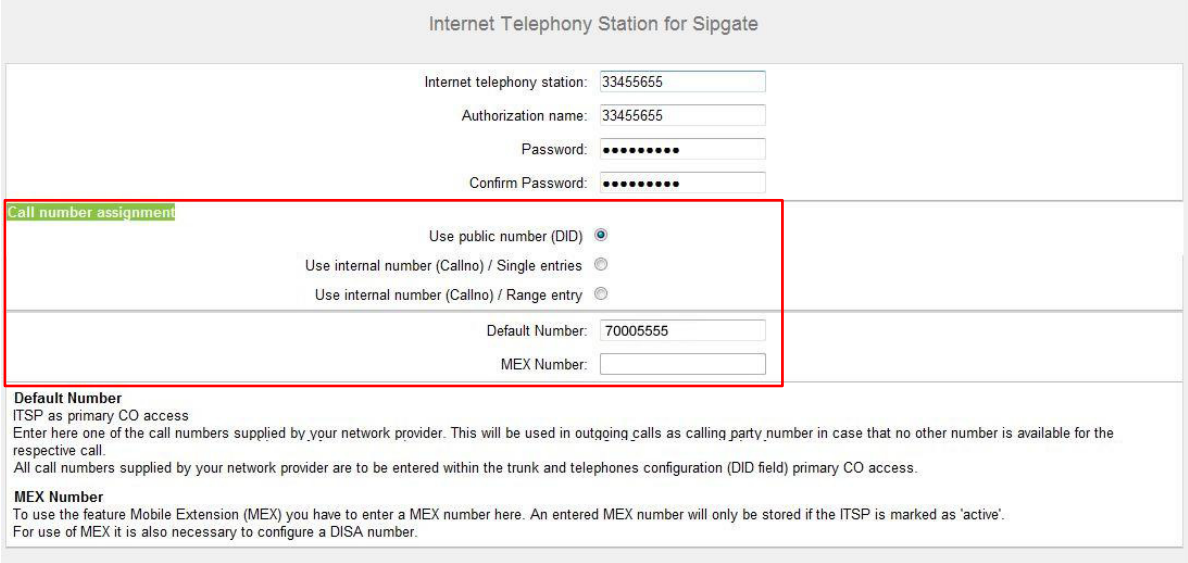
13) Geben Sie im Feld **Autorisierungsname** den Autorisierungsnamen ein. Die Daten haben Sie von Ihrem ITSP erhalten. Haben Sie keinen Autorisierungs-

namen erhalten, geben Sie die gleichen Daten wie unter **Internet-Telefonie-Teilnehmer** ein.

14) Geben Sie in den Feldern **Neues Kennwort** und **Kennwort wiederholen** das Kennwort an, dass Sie vom ITSP erhalten haben. Je nach ITSP werden hierfür unterschiedliche Bezeichnungen verwendet, wie z. B. SIP-Passwort oder SIP-Kennwort.

15) Zuordnung der Internet-Telefonie-Rufnummern - Möglichkeit 1:

Öffentliche Rufnummer (DuWa): die Internet-Telefonie-Rufnummern Ihres Internet-Telefonie-Teilnehmeranschlusses oder Internet-Telefonie-Anlagenanschlusses werden nicht hier bei der ITSP-Konfiguration, sondern bei der Teilnehmer-Konfiguration in den Feldern **DuWa** eingetragen.



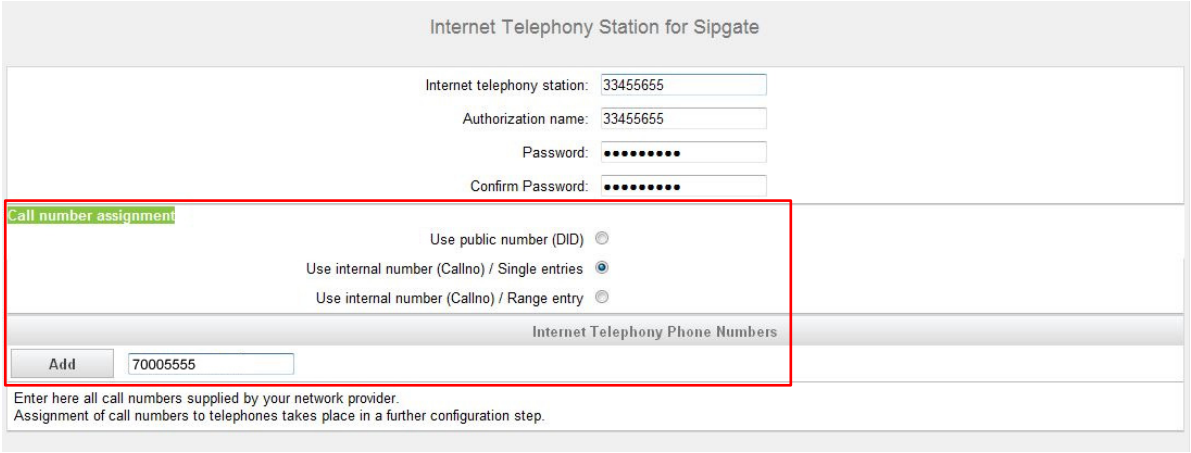
a) Wählen Sie im Bereich **Rufnummer assignment** das Optionsfeld **Öffentliche Rufnummer (DuWa)** aus.

b) Geben Sie unter **Standard-Rufnummer** die Rufnummer ein, die bei gehenden Anrufen für Teilnehmer verwendet werden soll, die keine eigene Rufnummer haben.

c) Falls Ihr ITSP das Leistungsmerkmal "Mobile Extension (MEX)" unterstützt, tragen Sie unter **MEX-Nummer** die vom ITSP zur Verfügung gestellte MEX-Nummer ein (8-stellig, nur Ziffern).

16) Zuordnung der Internet-Telefonie-Rufnummern - Möglichkeit 2:

Interne Nummer (Rufnr.) verwenden / Einzeleinträge: Sie haben einen Internet-Telefonie-Teilnehmeranschluss und als Internet-Telefonie-Rufnummern Einzelrufnummern erhalten (z. B. 70005555, 70005556,...). Diese Einzelrufnummern ordnen Sie anschließend den internen Rufnummern der Teilnehmer zu.



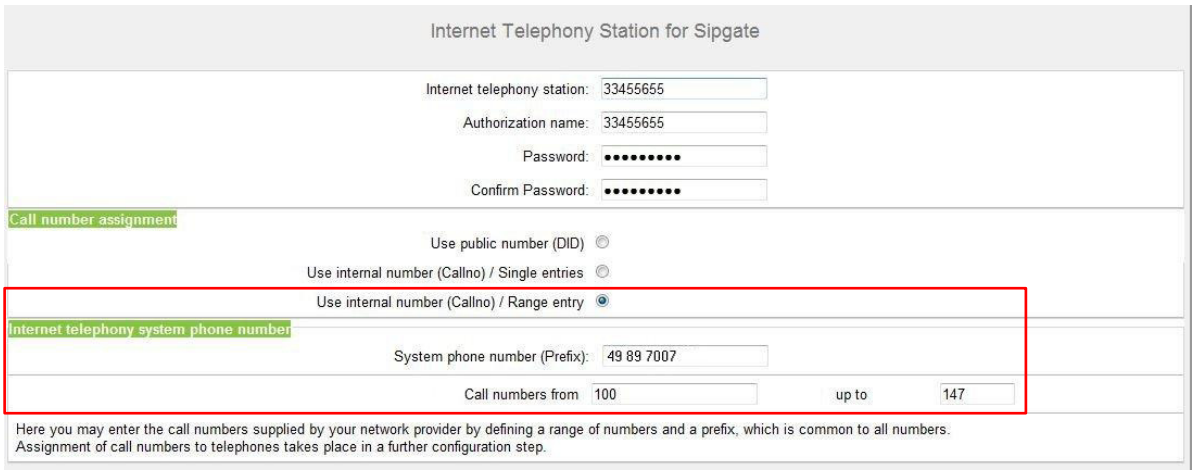
a) Wählen Sie im Bereich **Rufnummer assignment** das Optionsfeld **Interne Nummer (Rufnr.) verwenden / Einzeleinträge** aus.

b) Geben Sie im Bereich **Internet-Telefonie-Teilnehmerrufnummern** im Feld neben der Schaltfläche **Hinzufügen** eine der vom ITSP mitgeteilten Internet-Telefonie-Rufnummern ein und klicken Sie auf **Hinzufügen**.

c) Wenn Sie dem Account weitere Internet-Telefonie-Rufnummern zuordnen wollen, wiederholen Sie Schritt b).

17) Zuordnung der Internet-Telefonie-Rufnummern - Möglichkeit 3:

Interne Nummer (Rufnr.) verwenden / Bereichseintrag: Sie haben einen Internet-Telefonie-Anlagenanschluss und als Internet-Telefonie-Rufnummern ein Rufnummernband erhalten, z. B. (+49) 89 7007-100 bis (+49) 89 7007-147. Die Rufnummern aus dem Rufnummernband ordnen Sie anschließend den internen Rufnummern der Teilnehmer zu.



a) Wählen Sie im Bereich **Rufnummer assignment** das Optionsfeld **Interne Nummer (Rufnr.) verwenden / Bereichseintrag** aus.

b) Geben Sie unter **Anlagenrufnummer (Präfix)** die Anlagenrufnummer ein.

c) Geben Sie in den Feldern **Durchwahlband von** und **bis** das gewünschte Durchwahlband für den Internet-Telefonie-Teilnehmer ein. Standardmäßig ist 100 - 147 eingetragen.

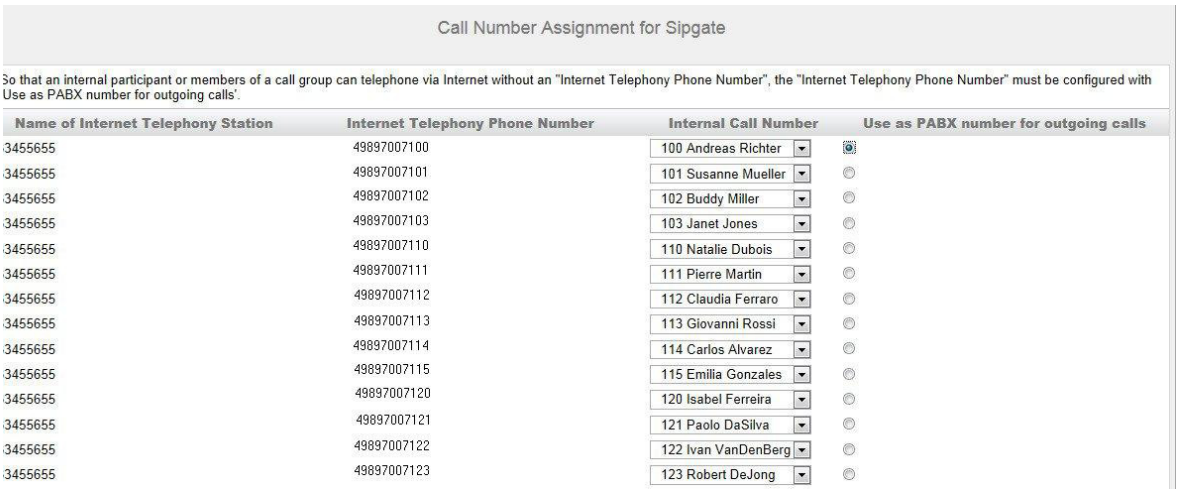
18) Klicken Sie auf **OK & Weiter**.

19) Wenn Sie weitere Accounts einrichten möchten, wiederholen Sie die Schritte 11 bis 18.

20) Klicken Sie auf **OK & Weiter**. Sie sehen eine Übersicht, welche Internet-Telefonie-Rufnummern welchen Accounts zugeordnet sind.

21) Ordnen Sie allen Internet-Telefonie-Rufnummern jeweils einer internen Rufnummer eines Teilnehmers zu.

Dieser Schritt entfällt, wenn Sie für die Zuordnung der Internet-Telefonie-Rufnummern die Möglichkeit 1 gewählt haben. Die Zuordnung treffen Sie in diesem Fall bei der Teilnehmer-Konfiguration im Feld **DuWa**.



a) Wählen Sie in der entsprechenden Zeile aus der Aufklappliste **interne Rufnummer** eine interne Rufnummer aus.

b) Sollen Teilnehmer ohne Internet-Telefonie-Rufnummer oder Mitglieder einer Rufgruppe externe Telefonate über das Internet führen dürfen, muss das Optionsfeld **Als gehende Anlagenrufnummer verwenden** aktiviert sein. Das Optionsfeld kann ausschließlich bei einer einzigen Internet-Telefonie-Rufnummer aktiviert sein.

22) Klicken Sie auf **OK & Weiter**. Hier sehen Sie nochmals die Übersicht der möglichen ITSP. Aktivierte ITSP sind in der Spalte **Provider aktivieren** mit einem Häkchen markiert. Mit **Restart ITSP** können Sie sich bei Verbindungsproblemen bei bereits aktivierten ITSP neu registrieren.

23) Klicken Sie auf **OK & Weiter**.

24) Geben Sie im Feld **Upstream bis zu (Kbit/s)** den Wert der Upload-Geschwindigkeit Ihrer Internet-Verbindung ein. Nicht zu verwechseln mit der Download-Geschwindigkeit!

INFO: Im Feld **Anzahl simultaner Internet-Telefongespräche** wird Ihnen die Anzahl der gleichzeitig zu führenden Internet-

Telefongespräche angezeigt. Wenn sich auf Grund der Netzauslastung die Gesprächsqualität verschlechtert, müssen Sie die Anzahl reduzieren.

25) Klicken Sie auf **OK & Weiter**.

26) Falls Sie bei der Einrichtung Ihres Internet-Zugangs die Dauerverbindung noch nicht aktiviert haben, können Sie das hier nachholen. Ohne Dauerverbindung können Sie keine Anrufe über das Internet empfangen. Ist die Dauerverbindung bereits eingerichtet, erscheinen die unter a) bis c) beschriebenen Felder nicht.

a) Aktivieren Sie unter **Dauerverbindung** das Optionsfeld **An**.

b) Legen Sie im Feld **Zwangstrennung um (Std:Min)** die Uhrzeit fest, zu der die Internet-Verbindung getrennt werden soll (z. B. 04:59).

c) Klicken Sie auf **OK & Weiter**.

27) Tragen Sie in der Spalte **Gewählte Ziffern** die gewünschten Sonderrufnummern ein.

Folgende Rufnummerneinträge sind gültig:

0 bis 9: erlaubte Ziffern

-: Feldtrennzeichen

X: beliebige Ziffer zwischen 0 bis 9

N: beliebige Ziffer zwischen 2 bis 9

Z: eine oder mehrere Ziffern folgen bis Wahlende

C: simulierter Wählton (kann max. 3 mal eingetragen werden)

28) Wählen Sie in der Spalte **Wählen über Provider** aus, ob die Sonderrufnummer über ISDN oder über einen ITSP gewählt werden soll. Es werden nur aktive ITSP angezeigt.

INFO: Stellen Sie sicher, dass Notrufnummern immer gewählt werden können. Falls Notrufnummern über einen Internet-Telefonie-Service-Provider gewählt werden sollen, muss der ITSP dies unterstützen.

29) Klicken Sie auf **OK & Weiter**. Es wird Ihnen der Status der ITSP angezeigt.

30) Klicken Sie auf **Weiter** und anschließend auf **Beenden**. Bitte durchlaufen Sie anschließend den Wizard **Amtsleitung ISDN / Analog / ITSP**, um die Priorisierung für die Amtsholung einzustellen (z. B. Amtsholung zuerst über ITSP und dann über ISDN).

9.2.1.3 Wie Sie eine vorkonfigurierte ITSP-Vorlage als neue Vorlage abspeichern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Sprachgateway**.
3) Klicken Sie im Menübaum auf **Internet-Telefonie Service Provider**.
4) Klicken Sie auf die Registerkarte **Internet-Telefonie Service Provider hinzufügen**.
5) Wählen Sie aus der Auswahlliste **Template verwenden** die gewünschte ITSP-Vorlage aus.
6) Geben Sie im Feld **Provider-Name** den gewünschten Namen der neuen ITSP-Vorlage ein.
7) Passen Sie die Werte der Vorlage an Ihre Belange an. Die Erklärung der Werte finden Sie unter *Sprachgateway > Internet-Telefonie Service Provider*.
8) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9.2.1.4 Wie Sie eine vorkonfigurierte ITSP-Vorlage anpassen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Sprachgateway**.
3) Klicken Sie im Menübaum auf **Internet-Telefonie Service Provider**.
4) Klicken Sie im Menübaum auf die gewünschte ITSP-Vorlage.
5) Klicken Sie auf die Registerkarte **Internet-Telefonie Service Provider ändern**.
6) Passen Sie die Werte der Vorlage an Ihre Belange an. Die Erklärung der Werte finden Sie unter *Sprachgateway > Internet-Telefonie Service Provider*.

INFO: Mit der Schaltfläche **Default-Werte zurücksetzen** können Sie Ihre geänderten Werte auf die Standard-Werte der Vorlage zurücksetzen. Ist der ITSP der Vorlage bereits aktiviert, werden alle Accounts des ITSP sofort abgemeldet und mit den Standard-Werten neu registriert.

INFO: Mit der Schaltfläche **Aktualisieren** können Sie die Standard-Werte auf den neuesten Stand bringen, sofern ein Software-Update durchgeführt wurde und es in diesem Update aktuellere Standard-Werte für diese Vorlage gibt.

---

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9.2.1.5 Wie Sie eine vorkonfigurierte ITSP-Vorlage manuell aktualisieren

Voraussetzungen

- Der ITSP dieser Vorlage ist aktiviert.
- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Sprachgateway**.

3) Klicken Sie im Menübaum auf **Internet-Telefonie Service Provider**.

4) Klicken Sie im Menübaum auf die gewünschte ITSP-Vorlage.

5) Klicken Sie auf die Registerkarte **Internet-Telefonie Service Provider ändern**.

6) Notieren Sie sich die Werte der Vorlage, die Sie gegenüber den Standard-Werten geändert haben (z. B. mit Hilfe eines Screenshots).

7) Klicken Sie auf **Aktualisieren**. Die Standard-Werte der Vorlage werden aktualisiert, sofern ein Software-Update des Systems durchgeführt wurde und es in diesem Update aktuellere Standard-Werte für diese Vorlage gibt.

8) Passen Sie die Werte der Vorlage wieder an Ihre Belange an. Die Erklärung der Werte finden Sie unter *Sprachgateway > Internet-Telefonie Service Provider*.

> ***INFO:*** Mit der Schaltfläche **Default-Werte zurücksetzen** können Sie Ihre geänderten Werte auf die Standard-Werte der Vorlage zurücksetzen. Dabei werden alle Accounts des ITSP sofort abgemeldet und mit den Standard-Werten neu registriert.

9) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9.2.2 STUN, Simple Traversal of UDP through NAT

STUN ermittelt beim Betrieb des Kommunikationssystems hinter einem NAT-Router die eigene öffentliche IP-Adresse/Port, die für einige ITSP erforderlich ist. Die Funktionalität wird im Internet auf STUN-Servern bereitgestellt, deren Adressen entsprechend in der Konfiguration des Kommunikationssystems hinterlegt sein müssen.

Der benötigte STUN-Modus ist abhängig von der ITSP-Infrastruktur und dem verwendeten Internet-Router. STUN wird nicht benötigt, wenn der ITSP NAT

Traversal auflöst, indem er Infrastruktur-Komponenten im Provider-Netzwerk verwendet wie den Session Border Controller (SBC).

Folgende STUN-Modi können am Kommunikationssystem eingestellt werden:

- **Automatisch (Standard)**
  Ist kein ITSP aktiv, ist STUN in diesem Modus komplett ausgeschaltet. Ist ein ITSP aktiv, bestimmt STUN den verwendeten Firewall-Typ (NAT-Typ) beim Systemstart und kann während des Betriebs Änderungen an den IP-Adressen erkennen. Abhängig vom festgestellten NAT-Typ ändert STUN bestimmte Parameter in den SIP-Nachrichten.

  INFO: Symmetric NAT wird nicht unterstützt.

- **Immer**
  STUN ist immer aktiv. Abhängig vom festgestellten NAT-Typ sind einige Parameter in den SIP-Nachrichten angepasst.
- **Statische IP verwenden**
  DSL-Modem oder Internet-Router nutzen eine statische IP-Adresse (öffentliche IP-Adresse) und der ITSP fordert eine statische IP-Authentifizierung. Die vom Modem oder Router verwendete statische IP-Adresse und Port müssen zusätzlich angegeben werden.
- **Router behält Port bei**
  Die öffentliche IP-Adresse wird über STUN ermittelt. Der Port wird unverändert in die SIP-Nachrichten eingetragen.

9.2.2.1 Wie Sie den STUN-Modus festlegen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

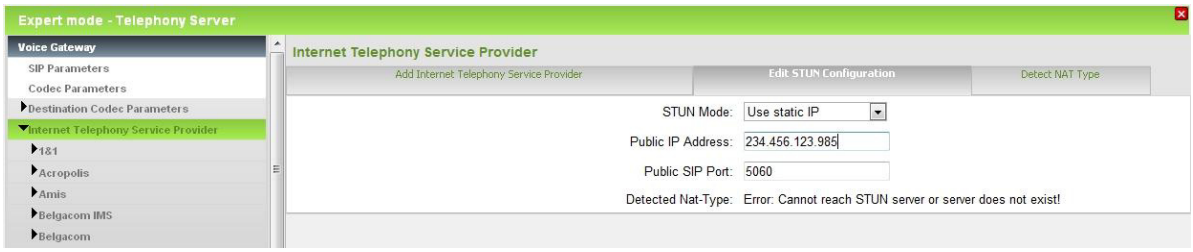
Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Sprachgateway**.

3) Klicken Sie im Menübaum auf **Internet-Telefonie Service Provider**.

4) Klicken Sie auf die Registerkarte **STUN-Konfiguration ändern**.



5) Wählen Sie aus der Aufklappliste **STUN-Modus** den gewünschten STUN-Modus aus.

6) Wenn Sie den STUN-Modus **Statische IP verwenden** ausgewählt haben, geben Sie unter **öffentliche IP-Adresse** und **öffentlicher SIP-Port** die statische IP-Adresse und den Port des DSL-Modems oder des Internet-Routers ein.

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9.3 Amtszugang über digitale und analoge Leitungen

Der Amtszugang über ISDN-Leitungen oder analoge Leitungen verbindet die Hardwareplattformen mit dem öffentlichen Netz (PSTN).

Wizards erleichtern die Konfiguration eines ISDN-Amtszugangs oder eines analogen Amtszugangs.

9.3.1 Leitungen

Leitungen verbinden die Hardwareplattformen mit dem öffentlichen Netz (PSTN). Jeder Leitung muss eine Richtung zugewiesen sein, über die man der Leitung verschiedene Eigenschaften zuordnen kann.

Standardmäßig sind allen Leitungen eine Leitungskennzahl und eine Richtung zugewiesen. Diese Zuordnungen können vom Administrator geändert werden.

Bei einem ISDN-Amtsanschluss spricht man bei Leitungen auch von B-Kanälen.

Leitungskennzahl

Anhand der Leitungskennzahl wird vom Kommunikationssystem die der Leitungskennzahl zugeordnete Leitung belegt. Die Leitungskennzahl dient auch zum Programmieren einer Leitungstaste oder zum Prüfen einer Leitung.

MSN-Zuordnung

Der Service Provider vergibt zu jedem ISDN-Mehrgeräteanschluss (PMP, Point-to-Multipoint) eine oder mehrere MSN (Multiple Subscriber Number). Diese können direkt einer Leitung zugeordnet werden.

Systemrufnummern

Systemrufnummern beinhalten das internationale Präfix, die Länder- und Ortsvorwahl und die Anlagenrufnummer bzw. eine oder mehrere MSN.

ISDN-Protokoll

Das verwendete ISDN-Protokoll richtet sich nach der Länderkennzahl. Es sollte nur geändert werden, falls die PSTN-Anbindung ausdrücklich ein bestimmtes, abweichendes Protokoll erfordert. Es steht eine große Anzahl von Protokoll-Templates zur Verfügung, die an die eigenen Belange angepasst werden können. Die dafür notwendigen Informationen erhalten Sie von Ihrem Service Provider.

B-Kanal-Belegungsmodus

Einzelne B-Kanäle einer ISDN-Leitung lassen sich für gehenden und/oder kommenden Verkehr sperren.

Es sind folgende B-Kanal-Belegungsmodi möglich:

- nur gehend
- nur kommend
- gehend und kommend (Standard)

Der B-Kanal-Belegungsmodus wird nur dann ausgewertet, wenn das Kommunikationssystem einen B-Kanal vorschlagen muss. Dies gilt in folgenden Situationen:

S_2 gehend:	Hierbei muss das Kommunikationssystem einen B-Kanal vorschlagen.
S_2 kommend:	Die Gegenstelle ist verpflichtet, einen B-Kanal vorzuschlagen. Dieser B-Kanal wird vom Kommunikationssystem ohne Prüfung der Einstellung übernommen. Die Einstellung hat somit keinen Einfluss.
S_0 gehend:	Da das Kommunikationssystem keinen B-Kanal vorgibt (any channel), hat die Einstellung keinen Einfluss.
S_0 kommend:	Wenn die Gegenstelle das Gespräch ohne B-Kanal-Vorgabe aufbaut, so wird vom Kommunikationssystem ein B-Kanal vorgeschlagen. Für diesen Vorschlag wird der eingestellte B-Kanal-Belegungsmodus beachtet.

Wahlverfahren für analoge Amtsleitungen (HKZ)

Das Wahlverfahren wird vom Kommunikationssystem automatisch bei jeder Leitungsbelegung erkannt. Für spezielle Fälle kann das Wahlverfahren auch direkt auf das Mehrfrequenzwahlverfahren (MFV) oder das Impulswahlverfahren (IWV) eingestellt werden.

9.3.1.1 Wie Sie den ISDN-Amtszugang konfigurieren

Mit dem Wizard **Amtsleitung ISDN / Analog / ITSP** konfigurieren Sie den ISDN-Amtszugang. Je nach den im Kommunikationssystem vorhandenen Ports für Amtsleitungen (ISDN oder analog) durchläuft der Wizard unterschiedliche Schritte.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.
- Das Kommunikationssystem ist an eine ISDN-Amtsleitung angeschlossen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Zentrale Telefonie**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Amtsleitung ISDN / Analog / ITSP** zu starten. Der Wizard zeigt eine Übersicht der Box(en), Slots und S_0-Ports.

4) Geben Sie im Feld **Ländervorwahl** die Ländervorwahl ein, z. B. `49` für Deutschland oder `1` für USA.

5) Geben Sie im Feld **Ortsnetzkennzahl** die Ortsvorwahl ein, z. B. 89 für München.

6) Wenn es sich um einen Anlagenanschluss handelt, geben Sie im Feld **Anlagenrufnummer** die Anlagenrufnummer Ihres Amtsanschlusses ein, z. B. 7007 (Ihre Anschlussnummer).

7) Ändern Sie das Feld **Internationales Präfix** nur wenn nötig. Für Deutschland gilt `00`, für USA `011`).

Bei Telefonaten ins Ausland wird der Telefonnummer das internationale Präfix und die Ländervorwahl vorangestellt, z. B. von Deutschland nach USA `00-1` und von USA nach Deutschland `011-49`.

8) Klicken Sie auf **OK & Weiter**.

9) Wählen Sie für den betreffenden Anschluss (Box, Slot und S_0-Port) eine der folgenden Anschlussarten:

- Wenn Sie einen Anlagenanschluss konfigurieren möchten, aktivieren Sie das Optionsfeld **Anlagenanschluss**.
- Wenn Sie einen Mehrgeräteanschluss konfigurieren möchten, aktivieren Sie das Optionsfeld **Mehrgeräteanschluss**.

10) Klicken Sie auf **OK & Weiter**.

11) Wenn es sich um einen Mehrgeräteanschluss handelt, geben Sie für den betreffenden Anschluss (Box, Slot und S_0-Port) die MSN ein und klicken Sie auf **OK & Weiter**.

12) Belassen Sie die Einstellung des Kontrollkästchens **Keine Telefonie über Internet** und klicken Sie auf **Überspringen**.

13) Wählen Sie in der Aufklappliste **Zuerst über** den bevorzugten Amtszugang und klicken Sie auf **OK & Weiter**.

14) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

9.3.1.2 Wie Sie einen analogen Amtszugang konfigurieren

Mit dem Wizard **Amtsleitung ISDN / Analog / ITSP** konfigurieren Sie den analogen Amtszugang.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.
- Das Kommunikationssystem ist an eine analoge Amtsleitung angeschlossen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Zentrale Telefonie**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Amtsleitung ISDN / Analog / ITSP** zu starten. Der Wizard zeigt eine Übersicht der Box(en), Slots und analogen Ports.

4) Geben Sie im Feld **Ländervorwahl** die Ländervorwahl ein, z. B. `49` für Deutschland oder `1` für USA.

5) Geben Sie im Feld **Ortsnetzkennzahl** die Ortsvorwahl ein, z. B. 89 für München.

6) Wenn es sich um einen Anlagenanschluss handelt, geben Sie im Feld **Anlagenrufnummer** die Anlagenrufnummer Ihres Amtsanschlusses ein, z. B. 7007 (Ihre Anschlussnummer).

7) Ändern Sie das Feld **Internationales Präfix** nur wenn nötig. Für Deutschland gilt `00`, für USA `011`).

Bei Telefonaten ins Ausland wird der Telefonnummer das internationale Präfix und die Ländervorwahl vorangestellt, z. B. von Deutschland nach USA `00-1` und von USA nach Deutschland `011-49`.

8) Klicken Sie auf **OK & Weiter**.

9) Klicken Sie auf **ISDN überspringen**.

10) Belassen Sie die Einstellung des Kontrollkästchens **Keine Telefonie über Internet** und klicken Sie auf **Überspringen**.

11) Wählen Sie aus der Aufklappliste **Protokoll** das Protokoll für die Anzeige der Rufnummer (Service-Provider-abhängig) aus:

- Wenn Sie Frequency Shift Keying verwenden möchten, wählen Sie **FSK**.
- Wenn Sie das Mehrfrequenzwahlverfahren verwenden möchten, wählen Sie **MFW**.
- Wenn Sie keine Rufnummernanzeige verwenden möchten, wählen Sie **keine**.

12) Klicken Sie auf **OK & Weiter**.

13) Klicken Sie auf **Bearbeiten**, um Eigenschaften der betreffenden Leitung zu konfigurieren. Ändern Sie bei Bedarf **Wahlverfahren**, **Amtsruferkennung**, **Flash**, **Leitungslänge** und **Flags** und klicken Sie auf **OK**.

14) Klicken Sie auf **OK & Weiter**.

15) Klicken Sie auf **Überspringen** und auf **OK & Weiter**.

16) Wählen Sie in der Aufklappliste **Zuerst über** den bevorzugten Amtszugang und klicken Sie auf **OK & Weiter**.

17) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

9.3.1.3 Wie Sie alle Leitungen anzeigen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Leitungen/Vernetzung**.
3) Klicken Sie im Menübaum auf **Leitungen/Vernetzung > Leitungen**. Ihnen werden abhängig vom Ausbau des Kommunikationssystems alle möglichen Leitungen inkl. Leitungskennzahl und Richtung angezeigt.

9.3.1.4 Wie Sie eine einzelne Leitung anzeigen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Leitungen/Vernetzung**.
3) Navigieren Sie im Menübaum unter **Leitungen/Vernetzung > Leitungen > ...** zur gewünschten Leitung. Ihnen wird die am Kommunikationssystem angeschlossene Leitung inkl. Leitungskennzahl und Richtung angezeigt.
4) Klicken Sie auf **OK**.

9.3.1.5 Wie Sie eine Leitungskennzahl ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Leitungen/Vernetzung**.
3) Navigieren Sie im Menübaum unter **Leitungen/Vernetzung > Leitungen > ...** zur gewünschten Leitung.
4) Klicken Sie auf die Registerkarte **Leitung ändern**.
5) Geben Sie im Feld **Kennzahl** den gewünschten Wert ein.

INFO: Ist als Kennzahl kein Wert eingetragen, hat diese Leitung keine Leitungskennzahl.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9.3.1.6 Wie Sie eine MSN einer Leitung zuweisen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Leitungen / Vernetzung**.

3) Klicken Sie im Menübaum auf **Leitungen / Vernetzung > MSN zuweisen**.

4) Klicken Sie im Menübaum unter **MSN zuweisen** auf den Eintrag, den Sie bearbeiten möchten.

5) Geben Sie die **MSN** ein.

6) Wählen Sie in der Aufklappliste die **Leitung**, die Sie zuweisen möchten.

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9.3.1.7 Wie Sie das ISDN-Protokoll ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Leitungen / Vernetzung**.

3) Navigieren Sie im Menübaum unter **Leitungen/Vernetzung > Leitungen > ...** zum gewünschten Port.

4) Klicken Sie auf die Registerkarte **ISDN-Flags ändern**.

5) Wählen Sie im Bereich **Protokoll: Beschreibung** in der Aufklappliste das gewünschte Protokoll aus.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9.3.1.8 Wie Sie den B-Kanal-Belegungsmodus ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Leitungen / Vernetzung**.

3) Navigieren Sie im Menübaum unter **Leitungen/Vernetzung > Leitungen > ...** zum gewünschten Port.

4) Klicken Sie auf die Registerkarte **B-Kanal ändern**.

5) Deaktivieren Sie pro Kanal die Kontrollkästchen in den Spalten **gehend** und **kommend** nach Ihren Wünschen.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9.3.1.9 Wie Sie das Wahlverfahren ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Leitungen / Vernetzung**.

3) Navigieren Sie im Menübaum unter **Leitungen/Vernetzung > Leitungen > ...** zum gewünschten Port.

4) Klicken Sie auf die Registerkarte **HKZ-Flags ändern**.

5) Stellen Sie das Mehrfrequenzwahlverfahren (MFV) oder das Impulswahlverfahren (IWV) ein.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9.3.2 Richtungen

Über Richtungen können Leitungen (B-Kanäle) gebündelt werden. Für jedes Leitungsbündel (= Richtung) können eigene Parameter konfiguriert werden.

Jeder Leitung kann genau eine Richtung zugeordnet werden. Standardmäßig sind allen Leitungen die Richtung 1 zugewiesen.

Für jede Richtung kann ein Name und eine Richtungskennzahl vergeben werden.

INFO: Richtungskennzahlen sind für gehende Amtsbelegungen nur wirksam, wenn LCR nicht aktiv ist.

B-Kanalaufteilung

Eine Teilung der B-Kanäle auf verschiedene Leitungsbündel nennt man auch B-Kanalaufteilung. Für ISDN-Amtsanschlüsse mit vielen B-Kanälen, wie z. B. S_{2M}-Anschlüsse, kann eine Aufteilung der B-Kanäle auf verschiedenen Leitungsbündel sinnvoll sein.

Bei gehenden Gesprächen werden dann nur B-Kanäle ausgewählt, die in dem Leitungsbündel enthalten sind (z. B. über Richtungskennzahl ausgewähltes Leitungsbündel, Überlaufbündel oder über LCR ausgewähltes Leitungsbündel).

Kommende Gespräche werden immer unabhängig vom Leitungsbündel akzeptiert. Im Regelfall wird der vom Partner angebotene B-Kanal belegt. Daher muss die im System konfigurierte B-Kanalaufteilung auch auf der Partner-Seite (Anlage oder öffentliches Netz) unterstützt werden. Ist das nicht der Fall, kann die korrekte Zuordnung des Rufes zum entsprechenden Leitungsbündel nicht garantiert werden.

Richtungstaste

Ein Teilnehmer kann am Telefon eine Richtungstaste programmieren. Eine Richtungstaste ist für gehende Anrufe reserviert. Über Richtungstasten getätigte Anrufe unterliegen den Stufen und Regeln der COS-Wahlkontrolle.

Nachdem der Teilnehmer eine Richtungstaste drückt (oder eine Richtungskennzahl wählt), belegt das Kommunikationssystem zum Verbindungsaufbau eine verfügbare Leitung, die der entsprechenden Richtung zugeordnet ist. Das Telefon zeigt die Leitungsnummer im Display an. Sind alle Leitungen der Richtung belegt, leuchtet die entsprechende LED, auch bei erfolgreichem Überlauf.

Überlaufrichtung bei deaktiviertem LCR

Der Administrator kann für jede Richtung eine Überlaufrichtung festlegen. Sind bei einem Belegungsversuch alle Leitungen einer Richtung belegt, so wird die Suche unter allen Leitungen dieser Überlaufrichtung fortgesetzt. Sind auch in der Überlaufrichtung alle Leitungen belegt, erfolgt kein weiterer Überlauf.

Überlaufrichtung bei aktiviertem LCR

Der Administrator kann im Rahmen der LCR-Konfiguration bis zu 16 Einträge je Wegetabelle konfigurieren, die im Sinne eines Überlaufes nacheinander abgearbeitet werden.

Belegungsart

Für gehende Richtungsbelegung kann der Administrator durch die Belegungsart festlegen, nach welchem Kriterium das Kommunikationssystem eine verfügbare Leitung in der entsprechenden Richtung sucht:

- zyklisch:
  Nach der zuletzt gehend belegten Leitung - die Suche beginnt bei der nächsthöheren Leitungsnummer, bezogen auf die zuletzt gehend belegte Leitung in dieser Richtung. Dadurch werden alle Leitungen etwa gleich häufig verwendet.
- linear:
  Immer die erste freie Leitung - die Suche beginnt bei der niedrigsten Leitungsnummer, die dieser Richtung zugeordnet ist.

Anlagenrufnummer kommend und gehend

Der Administrator kann die Anlagenrufnummer kommend und die Anlagenrufnummer gehend getrennt festlegen. Damit kann die eigene Rufnummer bei gehenden Gesprächen anders darstellt werden als sie für die Erreichbarkeit bei kommenden Gesprächen benötigt wird. Die Anteile für Ländervorwahl, Ortsnetzkennzahl und Anlagenrufnummer sind dabei jeweils getrennt einzutragen. Unterschiedliche Einträge bei der Anlagenrufnummer kommend und gehend setzen die Verfügbarkeit des Leistungsmerkmal "CLIP no screening" im Amt voraus. Ist keine Anlagenrufnummer gehend konfiguriert, verwendet das Kommunikationssystem stets die Daten der Anlagenrufnummer kommend.

Bei einer kommenden Belegung auf einer ISDN-Leitung blendet das Kommunikationssystem aus der empfangenen Rufnummer die Anteile für die Anlagenrufnummer kommend entsprechend dem empfangenen Rufnummerntyp (Type Of Number = TON, siehe Tabelle unter Rufnummernübermittlung) linksbündig aus und interpretiert den verbleibenden Teil als Durchwahlnummer. Bei Rufnummerninformationen an das PSTN setzt das Kommunikationssystem die Anteile der Anlagenrufnummer gehend entsprechend dem konfigurierten Rufnummerntyp gehend automatisch als führenden Teil der Rufnummer ein. Der Anteil der Anlagenrufnummer muss am Amtsanschluss in Deutschland ohne Ortsnetzkennzahl und ohne Abwurf-Kennziffer (0) angegeben werden.

Rufnummernübermittlung

Die Rufnummer, die zum PSTN und zum Empfänger gesendet wird, kann sich folgendermaßen zusammensetzen:

Type Of Number (TON), gehend	zum PSTN übermittelte Rufnummer
Unbekannt TON=Unknown	nur Durchwahlnummer (Standardeinstellung)
Anlagenrufnummer TON=Subscriber	Anlagenrufnummer + Durchwahlnummer

Type Of Number (TON), gehend	zum PSTN übermittelte Rufnummer
Ortsnetzkennzahl TON=National	Ortsnetzkennzahl + Anlagenrufnummer + Durchwahlnummer
Ländervorwahl TON=International	Ländervorwahl + Ortsnetzkennzahl + Anlagenrufnummer + Durchwahlnummer
Intern TON=Intern	nur für vernetzes System: bei einem geschlossenen Rufnummernplan darf kein Nummern-Präfix ergänzt werden. Hier wird eine Rufnummernergänzung unterdrückt.

Weiterhin besteht die Möglichkeit anzugeben, welche Rufnummerninformation von dem wählenden Teilnehmer an den Zielteilnehmer gesendet werden soll.

Rufnummertyp	zum PSTN übermittelte Rufnummer
Intern	Hier wird nur eine Information über die interne Rufnummer mitgesendet. Ist der Zielteilnehmer Extern, wird entweder keine oder die Vermittlungsplatz-Rufnummer gesendet. Bei internen Zielteilnehmern kann die interne Rufnummer angezeigt werden.
Durchwahl	Hier wird nur eine Information über die DuWa-Nummer versendet. Bei internen Zielteilnehmern in einem anderen Knoten fehlt für eine Displayanzeige die interne Rufnummer. Für externe Ziele ist die Rufnummerninformation ausreichend.
Intern / DuWa	In einer Vernetzung ist es sinnvoll diese Einstellung zu wählen. Dem Zielteilnehmer werden sowohl die interne als auch die DuWa-Rufnummer gesendet. Wird in der Vernetzung ein interner Teilnehmer gerufen, kann diesem Teilnehmer die interne Rufnummer des Rufers angezeigt werden. Hat der interne Zielteilnehmer beispielsweise eine Anrufumleitung an ein externes Ziel aktiviert, so kann in diesem Fall eine DuWa-Rufnummer mitgesendet werden.

Zusätzlich kann die gewünschte Behandlung des Richtungspräfix konfiguriert werden:

- Kommender Ruf
  Die Anrufernummer wird bei der Weitergabe zum S0-Bus um die Richtungskennzahl ergänzt (-> wählbares Format für Rückruf) bzw. transparent durchgereicht. Standard: aktiviert.
- Gehender Ruf
  Die Darstellung der gewählten Rufnummer am Systemtelefon erfolgt mit bzw. ohne Richtungspräfix. Standard: aktiviert.

Zweite Amtskennziffer

Eine zweite Amtskennziffer wird dann definiert, wenn das Kommunikationssystem eine Unteranlage eines anderen Kommunikationssystems ist oder mit mehreren anderen Kommunikationssystemen vernetzt ist. Sie ist nur für Vernetzungs-Richtungen (Richtungsart=PABX) relevant. In diesem Fall dient die zweite Amtskennziffer als Belegungskennzahl für die Hauptanlage. Innerhalb einer Vernetzung sind die Kennzahlen für die Amtsbelegung, die Richtungskennzahl(en) und die zweite Amtskennziffer einheitlich zu konfigurieren. Standard in Deutschland ist 0.

9.3.2.1 Wie Sie die Richtungszuordnung ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Leitungen/Vernetzung**.

3) Navigieren Sie im Menübaum unter **Leitungen/Vernetzung > Leitungen > ...** zur gewünschten Leitung.

4) Klicken Sie auf die Registerkarte **Leitung ändern**.

5) Wählen Sie aus der Aufklappliste **Richtung** die Richtung aus, die Sie der Leitung zuweisen möchten.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9.3.2.2 Wie Sie den Richtungsnamen ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Leitungen/Vernetzung**.

3) Klicken Sie im Menübaum auf **Leitungen/Vernetzung > Richtung**.

4) Klicken Sie im Menübaum unter **Richtung** auf den Eintrag, den Sie bearbeiten möchten.

5) Geben Sie im Feld **Richtungsname** den gewünschten Wert ein.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9.3.2.3 Wie Sie die Richtungskennzahl ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

INFO: Richtungskennzahlen sind nur wirksam, wenn LCR nicht aktiv ist.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Leitungen/Vernetzung**.
3) Klicken Sie im Menübaum auf **Leitungen/Vernetzung > Richtung**.
4) Klicken Sie im Menübaum unter **Richtung** auf den Eintrag, den Sie bearbeiten möchten.
5) Geben Sie im Feld **Richtungskennzahlen** den gewünschten Wert ein.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9.3.2.4 Wie Sie eine Überlaufrichtung bei deaktiviertem LCR konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Leitungen / Vernetzung**.
3) Klicken Sie im Menübaum auf **Leitungen / Vernetzung > Richtung**.
4) Klicken Sie im Menübaum unter **Richtung** auf den Eintrag, den Sie bearbeiten möchten.
5) Wählen Sie in der Aufklappliste **Überlaufrichtung** den gewünschten Eintrag.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9.3.2.5 Wie Sie eine Überlaufrichtung bei aktiviertem LCR konfigurieren

Bei aktiviertem LCR erfolgt die Überlaufbehandlung durch sukzessive Abarbeitung der einzelnen Einträge einer LCR-Wegetabelle im Rahmen der LCR-Konfiguration (siehe *LCR (Least Cost Routing, Leitweglenkung)*).

9.3.2.6 Wie Sie die Belegungsart konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Leitungen/Vernetzung**.

3) Klicken Sie im Menübaum auf **Leitungen/Vernetzung > Richtung**.

4) Klicken Sie im Menübaum unter **Richtung** auf die Richtung, die Sie bearbeiten möchten.

5) Klicken Sie auf die Registerkarte **Richtungsparameter ändern**.

6) Wählen Sie in der Aufklappliste **Belegungsart** entweder **zyklisch** oder **linear** aus.

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9.3.2.7 Wie Sie die Anlagenrufnummer kommend und gehend eintragen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Leitungen / Vernetzung**.

3) Klicken Sie im Menübaum auf **Leitungen / Vernetzung > Richtung**.

4) Klicken Sie im Menübaum unter **Richtung** auf den Eintrag, den Sie bearbeiten möchten.

5) Geben Sie im Bereich **Anlagenrufnummer kommend** in die Felder **Ländervorwahl**, **Ortsnetzkennzahl** und **Anlagenrufnummer** die entsprechenden Werte ohne führende Nullen ein.

6) Geben Sie im Bereich **Anlagenrufnummer gehend** in die Felder **Ländervorwahl**, **Ortsnetzkennzahl** und **Anlagenrufnummer** die entsprechenden Werte ohne führende Nullen ein.

7) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie die Teilnehmer-Rufnummer unterdrücken möchten, aktivieren Sie das Kontrollkästchen **TIn.-Ruf Nr. unterdrücken**.
- Wenn Sie die Teilnehmer-Rufnummer nicht unterdrücken möchten, deaktivieren Sie das Kontrollkästchen **TIn.-Ruf Nr. unterdrücken**.

8) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9.3.2.8 Wie Sie das Format der übermittelten Rufnummer konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Leitungen/Vernetzung**.
3) Klicken Sie im Menübaum auf **Leitungen/Vernetzung > Richtung**.
4) Klicken Sie im Menübaum unter **Richtung** auf die Richtung, die Sie bearbeiten möchten.
5) Klicken Sie auf die Registerkarte **Richtungsparameter ändern**.
6) Wählen Sie in der Aufklappliste **Nr.-Typ, gehend** das gewünschte Format der übermittelten Rufnummer aus.
7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9.3.2.9 Wie Sie die Art der übermittelten Rufnummer konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Leitungen/Vernetzung**.
3) Klicken Sie im Menübaum auf **Leitungen/Vernetzung > Richtung**.
4) Klicken Sie im Menübaum unter **Richtung** auf die Richtung, die Sie bearbeiten möchten.
5) Klicken Sie auf die Registerkarte **Richtungsparameter ändern**.
6) Wählen Sie in der Aufklappliste **Rufnummer Typ** den Eintrag **Intern**, **Durchwahl** oder **Intern/DuWa**.
7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9.3.2.10 Wie Sie das Richtungs-Präfix konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Leitungen/Vernetzung**.
3) Klicken Sie im Menübaum auf **Leitungen/Vernetzung > Richtung**.
4) Klicken Sie im Menübaum unter **Richtung** auf die Richtung, die Sie bearbeiten möchten.

5) Klicken Sie auf die Registerkarte **Richtungsparameter ändern**.

6) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie die Rufnummernanzeige für kommende Gespräche um die Richtungskennzahl ergänzen möchten, aktivieren Sie im Bereich **Richtungsflags** das Kontrollkästchen **Rtg.-Präfix ergänzen kommend**.
- Wenn Sie die Rufnummernanzeige für kommende Gespräche nicht um die Richtungskennzahl ergänzen möchten, deaktivieren Sie im Bereich **Richtungsflags** das Kontrollkästchen **Rtg.-Präfix ergänzen kommend**.
- Wenn Sie die Rufnummernanzeige für gehende Gespräche um die Richtungskennzahl ergänzen möchten, aktivieren Sie im Bereich **Richtungsflags** das Kontrollkästchen **Rtg.-Präfix ergänzen gehend**.
- Wenn Sie die Rufnummernanzeige für gehende Gespräche nicht um die Richtungskennzahl ergänzen möchten, deaktivieren Sie im Bereich **Richtungsflags** das Kontrollkästchen **Rtg.-Präfix ergänzen gehend**.

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9.3.2.11 Wie Sie eine Richtung für die Vernetzung definieren und eine zweite Amtskennziffer eintragen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Leitungen/Vernetzung**.

3) Klicken Sie im Menübaum auf **Leitungen/Vernetzung > Richtung**.

4) Klicken Sie im Menübaum unter **Richtung** auf den Eintrag, den Sie bearbeiten möchten.

5) Geben Sie im Feld **Amtskennziffer (2. AKZ)** den gewünschten Wert ein.

6) Klicken Sie auf die Registerkarte **Richtungsparameter ändern**.

7) Wählen Sie in der Aufklappliste **Richtungsart** den Eintrag **PABX** aus.

8) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9.3.3 Wähltonüberwachung

Beim Verbindungsaufbau über eine analoge Amtsleitung können die gewählten Ziffern erst zum Amt geschickt werden, wenn ein Wählton (Hörzeichen) erkannt wurde. Da die Zeit bis zum Eintreffen des Wähltons je nach Netzbetreiber und Netzzustand variiert, muss das Eintreffen des Wähltons überwacht werden.

Die Konfiguration der Wähltonüberwachungszeit und der Ziffernwahlzeit erfolgt mit dem Manager E.

Verzögerungszeit der Wähltonüberwachung

Die Überwachung des Wähltons kann sofort erfolgen oder erst nach einer Pause. In manchen Fällen müssen dem Teilnehmer nach Leitungsbelegung zusätzlich Töne eingespielt werden, z. B. um ihm mitzuteilen, dass eine Umleitung im Amt aktiv ist. Für diese Fälle kann eine Verzögerungszeit der Wähltonüberwachung (Pause vor Wahl, 1-9 Sekunden) programmiert werden. Die gewählten Ziffern werden erst nach Ablauf dieser Pause zum Amt geschickt.

INFO: Anmerkung für Brasilien:

Wird das MFV-Wahlverfahren von analogen Endgeräten aus verwendet in Verbindung mit analogen Amtsleitungen (TLAx und TML8W) und Impulswahlverfahren nach der Wähltonüberwachung, kann es Probleme mit der Wahlkontrolle geben, wenn die Ländervorwahl auf Brasilien eingestellt ist. In diesem Fall gehen die MFV-Signale von den analogen Endgeräten direkt zu den analogen Amtsleitungen. Alle MFV-Signale gehen verloren, die vor dem Empfang des Wähltons gewählt werden. Hier muss die automatische Wegesuche (LCR) für eine einwandfreie Funktion von Wahlverfahren und Wahlkontrolle des Endgeräts aktiviert sein.

Wähltonüberwachungszeit

Die Zeit, wie lange auf den Wählton gewartet werden soll, kann konfiguriert werden. Wird nach der konfigurierten Zeit kein Wählton erkannt, wird die Leitung außer Betrieb genommen. Das System überprüft in zyklischen Abständen, ob der Wählton erneut vorhanden ist. Ist dies der Fall, wird die betreffende Leitung wieder in Betrieb genommen.

Ziffernwahlzeit

Es kann eingestellt werden, wieviele Sekunden nach Erkennung des Wähltons die erste gewählte Ziffer zum Amt geschickt werden soll (Standard: 0 s).

Auswertung des zweiten Wähltons

Das Kommunikationssystem kann einen zusätzlichen Wählton (2. Hörzeichen) erkennen. Das ist relevant für öffentliche Netzbetreiber, die bei Auslandsgesprächen einen zweiten Wählton senden, z. B. für Belgien nach 00 und für Frankreich nach 16 bzw. 19. Für Deutschland ist diese Funktion nicht relevant.

9.3.3.1 Wie Sie die Verzögerungszeit der Wähltonüberwachung konfigurieren

Voraussetzungen

- Ein analoger Port mit dem analogen Amtszugang ist vorhanden.
- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Leitungen/Vernetzung**.

3) Klicken Sie im Menübaum auf **Leitungen/Vernetzung > Richtung**.

4) Klicken Sie im Menübaum unter **Richtung** auf die analoge Richtung, die Sie bearbeiten möchten.

5) Klicken Sie auf die Registerkarte **Richtungsparameter ändern**.

6) Wenn die Wähltonüberwachung sofort erfolgen soll, aktivieren Sie im Bereich **Pause vor Wahl** das Optionsfeld **Hörtonauswertung**.

7) Wenn die Wähltonüberwachung erst nach einer Verzögerungszeit erfolgen soll, wählen Sie im Bereich **Pause vor Wahl** die Verzögerungszeit in Sekunden aus.

8) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9.3.3.2 Wie Sie die Wähltonüberwachungszeit konfigurieren

Voraussetzungen

- Es ist eine analoge Amtsbaugruppe gesteckt.

Schritt für Schritt

1) Melden Sie sich auf dem Admin-PC am Manager E an.

2) Klicken Sie in der Menüleiste auf **Datei | Übertragen**.

3) Wählen Sie das Register **Kommunikation**.

4) Aktivieren Sie im Bereich **Zugang** das Optionsfeld je nach Anschlussart des Admin-PC an das Kommunikationssystem.

5) Aktivieren Sie das Optionsfeld **KDS lesen/schreiben** und klicken Sie auf **Anlage -> PC**.

6) Klicken Sie auf **OK** und der KDS wird vom Kommunikationssystem zum Manager E übertragen.

7) Klicken Sie nach erfolgreicher Übertragung auf **OK** und anschließend auf **Schließen**.

8) Klicken Sie im Manager E im Menübaum der Anlagensicht auf **Einstellungen > Systemparameter > Zeitparameter**.

9) Stellen Sie in der Liste unter **Wähltonüberwachungszeit** mit **Basis** und **Faktor** die Zeit ein, wie lange max. auf den Wählton gewartet werden soll (Standard: Basis = `1s`, Faktor = `10`).

10) Klicken Sie auf **Übernehmen**.

11) Klicken Sie in der Menüleiste auf **Datei | Übertragen**.

12) Wählen Sie das Register **Kommunikation**.

13) Klicken Sie auf **PC -> Anlage** und anschließend auf **OK**. Die Einstellungen werden an das Kommunikationssystem übertragen.

14) Klicken Sie abschließend auf **OK** und **Schließen**.

9.3.3.3 Wie Sie die Ziffernwahlzeit konfigurieren

Voraussetzungen

- Es ist eine analoge Amtsbaugruppe gesteckt.

Schritt für Schritt

1) Melden Sie sich auf dem Admin-PC am Manager E an.

2) Klicken Sie in der Menüleiste auf **Datei | Übertragen**.

3) Wählen Sie das Register **Kommunikation**.

4) Aktivieren Sie im Bereich **Zugang** das Optionsfeld je nach Anschlussart des Admin-PC an das Kommunikationssystem.

5) Aktivieren Sie das Optionsfeld **KDS lesen/schreiben** und klicken Sie auf **Anlage -> PC**.

6) Klicken Sie auf **OK** und der KDS wird vom Kommunikationssystem zum Manager E übertragen.

7) Klicken Sie nach erfolgreicher Übertragung auf **OK** und anschließend auf **Schließen**.

8) Klicken Sie im Manager E im Menübaum der Anlagensicht auf **Einstellungen > Systemparameter > Zeitparameter**.

9) Stellen Sie in der Liste unter **Zeit zur HT-Auswertung nach der Wahl Trunk-HKZ** mit **Basis** und **Faktor** die Zeit ein, nach wie vielen Sekunden nach Erkennung des Wähltons die erste gewählte Ziffer zum Amt geschickt werden soll (Standard: Basis = `10ms`, Faktor = `0`).

10) Klicken Sie auf **Übernehmen**.

11) Klicken Sie in der Menüleiste auf **Datei | Übertragen**.

12) Wählen Sie das Register **Kommunikation**.

13) Klicken Sie auf **PC -> Anlage** und anschließend auf **OK**. Die Einstellungen werden an das Kommunikationssystem übertragen.

14) Klicken Sie abschließend auf **OK** und **Schließen**.

9.3.3.4 Wie Sie die Auswertung des zweiten Wähltons aktivieren oder deaktivieren

Voraussetzungen

- Ein analoger Port mit dem analogen Amtszugang ist vorhanden.
- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Leitungen/Vernetzung**.

3) Klicken Sie im Menübaum auf **Leitungen/Vernetzung > Richtung**.

4) Klicken Sie im Menübaum unter **Richtung** auf die analoge Richtung, die Sie bearbeiten möchten.

5) Klicken Sie auf die Registerkarte **Richtungsparameter ändern**.

6) Wenn die Auswertung des zweiten Wähltons aktiviert werden soll, aktivieren Sie im Bereich **Richtungsflags** das Kontrollkästchen **Auswertung 2. Hörzeichen**.

7) Wenn die Auswertung des zweiten Wähltons deaktiviert werden soll, deaktivieren Sie im Bereich **Richtungsflags** das Kontrollkästchen **Auswertung 2. Hörzeichen /Leitungsüberwachung**.

8) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9.4 Priorisierung der Amtsholung bei aktiviertem LCR

Bei der Priorisierung der Amtsholung wird festgelegt in welcher Reihenfolge verschiedene Anbieter (ISDN/Analog oder ITSPs) ausgewählt werden.

Die Amtsholung geschieht normalerweise über die Vorwahl der Kennzahl "0". Innerhalb dieser Kennzahl werden (je nach Voreinstellung) verschiedene Anbieter priorisiert. So kann ein gehendes Gespräch zuerst über einen ITSP und, bei erfolgloser Amtsholung, danach über ISDN abgesetzt werden.

9.4.1 Wie Sie die Amtsholung priorisieren

Mit dem Wizard **Amtsleitung ISDN / Analog / ITSP** konfigurieren Sie die Reihenfolge der Amtsholung über ISDN/Analog und ITSPs.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.Verschiedene ITSPs sind eingerichtet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Zentrale Telefonie**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Amtsleitung ISDN / Analog / ITSP** zu starten. Der Wizard zeigt eine Übersicht der Box(en), Slots und analogen Ports.

4) Klicken Sie auf **OK & Weiter**.

5) Klicken Sie so oft auf **OK & Weiter** bis Sie auf das Fenster **Priorisierung für die Amtsholung** kommen.

6) Wählen Sie im Bereich **Versuche Amtsholung** in der Aufklappliste **Zuerst über** den bevorzugten Anbieter, über den das Kommunikationssystem als Erstes versucht eine freie Amtsleitung zu bekommen.

7) Wählen Sie in der Aufklappliste **Dann über** einen zweiten Anbieter, über den der nächste Versuch einer Amtsholung gemacht wird.

8) Wählen Sie in der nächsten Aufklappliste **Dann über** den dritten Anbieter, über den der Versuch einer Amtsholung gemacht wird.

9) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

10 Teilnehmer

Ein Teilnehmer ist ein am Kommunikationssystem angeschlossener Kommunikationspartner. In der Regel ist jedem Teilnehmer ein Endgerät zugeordnet (außer bei virtuellen Teilnehmern). Ein Endgerät ist z. B. ein Telefon, ein PC oder ein Fax-Gerät. Die Teilnehmer können auch Benutzer der UC Clients sein.

Es gibt folgende Arten von Teilnehmern:

- IP-Teilnehmer (auch IP-Clients genannt)
- SIP-Teilnehmer (eine Untergruppe der IP-Teilnehmer)
- UP0-Teilnehmer
- DECT-Teilnehmer
- ISDN-Teilnehmer
- Analoge Teilnehmer
- Mobility Teilnehmer (mobile Teilnehmer, siehe *Mobility*)
- Virtuelle Teilnehmer

Die Daten der Teilnehmer (Name, Rufnummer, Durchwahl, E-Mail-Adresse, usw.) können als XML-Datei während der Erstinstallation importiert werden (siehe *Individueller Rufnummernplan*). Zusätzlich können die Daten der Teilnehmer auch in eine XML-Datei exportiert werden (siehe *Export von Teilnehmerdaten*).

Lizenzverfahren für Teilnehmer

Alle Teilnehmer unterliegen der Lizenzierung. Zuerst werden die Teilnehmer während der Erstinstallation oder nachträglich über die Teilnehmer-Wizards eingerichtet. Nach erfolgreicher Einrichtung können die Teilnehmer intern miteinander telefonieren. Anschließend müssen die Teilnehmer-Lizenzen aktiviert und den Teilnehmern zugeordnet werden. Nach erfolgreicher Zuordnung können die Teilnehmer auch extern telefonieren.

Verwandte Themen

- Lizenzierung
- Mobility

10.1 Rufnummernplan

Ein Rufnummernplan ist eine Liste aller im Kommunikationssystem verfügbaren Rufnummern und Kennzahlen. Er beinhaltet u. a. interne Rufnummern, Durchwahlrufnummern und Gruppenrufnummern. Im Kommunikationssystem sind die Rufnummern und Kennzahlen mit Standardwerten vorbelegt. Diese Werte können aber bei Bedarf individuell angepasst werden.

Eventuell kann es beim Einrichten von Rufnummern oder Kennzahlen zu Fehlermeldungen kommen, wenn die gewünschte Nummer bereits belegt ist. Mit Hilfe

des Rufnummernplans kann geprüft werden, welche Rufnummern noch zu vergeben sind.

10.1.1 Standard-Rufnummernplan

Der Standardrufnummernplan beinhaltet alle Rufnummern und Kennzahlen, die im Kommunikationssystem mit Standardwerten vorbelegt sind.

Die Standardwerte können bei Bedarf geändert werden. Einige Rufnummern können zusätzlich komplett gelöscht werden, so dass sie in einer Rufnummernplan-Übersicht nicht mehr angezeigt werden.

Standard-Rufnummernplan für die Hardware-Plattformen und den Softswitch:

Art der Rufnummern	X1	X3/X5/X8/S	Aktion
Interne Teilnehmer-Rufnummern	11-30	100-742	löschbar
Teilnehmer-Durchwahlnummern	11 -30	100-742	löschbar
Gruppenrufnummern 1-90	31-40	350-439	löschbar
Gruppenrufnummern 91-800	-	nicht vorbelegt	
Leitungsrufnummern	700-703	ab 7801	löschbar
Richtungskennzahlen (Externkennzahlen):			nur änderbar
Rtg. 1 (Amt ISDN, analog)	0 = Welt / 9 = USA	0 = Welt / 9 = USA	
Rtg. 8 (UC Suite)	-	851	
Rtg. 12-15 (Amt ITSP)	nicht vorbelegt	855-858	
Rtg. 16 (Vernetzung)	nicht vorbelegt	859	
Platzkennzahl (Abwurfplatz) Intern	9 = Welt	9 = Welt	nur änderbar
	0 = USA	0 = USA	
Platzkennzahl (Abwurfplatz) Durchwahl	0 = Welt	0 = Welt	nur änderbar
	– = USA	– = USA	
Rufnummer für Online User	nicht vorbelegt	749	nur änderbar
Rufnummer für den Remote-Zugang	nicht vorbelegt	nicht vorbelegt	nur änderbar
Rufnummer für Sprachnachrichten			
UC Smart	351	351	nur änderbar
UC Suite	-	nicht vorbelegt	nur änderbar
Konferenz-Rufnummern	-	nicht vorbelegt	nur änderbar
Rufnummer für Parken	-	nicht vorbelegt	nur änderbar
AutoAttendant-Rufnummern	-	nicht vorbelegt	nur änderbar
Rufnummer für Vermittlungsplatz	9 = Welt	9 = Welt	nur änderbar
	0 = USA	0 = USA	

Art der Rufnummern	X1	X3/X5/X8/S	Aktion
Substitution für "*" (bei Kennzahlen)	75	75	löschbar
Substitution für "#" (bei Kennzahlen)	76	76	löschbar
Servicekennzahlen			nur änderbar

10.1.2 Individueller Rufnummernplan

Das Kommunikationssystem ermöglicht das Einrichten eines individuellen Rufnummernplans. Dazu können die Standardwerte der Rufnummern und Kennzahlen geändert werden. Bei einem Reload des Kommunikationssystems werden die Werte auf den Standard zurückgesetzt.

Folgende Aktionen sind dabei hilfreich:

- Standard-Rufnummern löschen: bis auf einige Ausnahmen (spezielle Standard-Rufnummern) können Standard-Rufnummern zusammenhängend gelöscht werden. Diese Rufnummern sind in der Tabelle des Standardrufnummernplans in der Spalte "Aktion" mit "löschbar" gekennzeichnet.
- Spezielle Standard-Rufnummern ändern: diese Rufnummern dürfen nicht gelöscht werden. Allerdings lassen sich die Werte dieser Rufnummern ändern. Diese Rufnummern sind in der Tabelle des Standardrufnummernplans in der Spalte "Aktion" mit "nur änderbar " gekennzeichnet.
- Rufnummern und Teilnehmerdaten importieren: über eine XML-Datei können Teilnehmerdaten während der Erstinstallation importiert werden. Dabei werden auch Rufnummer und Durchwahlrufnummer der Teilnehmer importiert. In der Regel wird das während der Erstinstallation durchgeführt.

Teilnehmerdatenimport über XML-Datei

Ein individueller Rufnummernplan kann über eine XML-Datei im UTF-8-Format während der Erstinstallation in das Kommunikationssystem importiert werden.

Das Administrationsprogramm OpenScape Business Assistant stellt unter **Service-Center > Dokumente > CSV-Vorlagen** die Datei `csv-templates.zip` zur Verfügung. Diese Zip-Datei enthält u.a. die folgenden Dateien inkl. Beschreibung.

- `portdata_xml_import_empty.xml`
  Diese Vorlage enthält Register ohne Beispieldatensätze. Es können z. B. mit Microsoft Excel neue Datensätze eingetragen werden.
- `portdata_xml_import_example.xml`
  Diese Vorlage enthält Register mit Beispieldatensätzen. Diese können z. B. mit Microsoft Excel überschrieben werden. Nicht benötigte Datensätzen sollten gelöscht werden.
- `portdata_xml_import_syntax.txt`
  Beschreibung in Deutsch und Englisch zum korrekten Anlegen der Datensätze.

10.1.2.1 Wie Sie Standard-Rufnummern löschen oder ändern

Sie können einige der Standard-Rufnummern löschen und anschließend über die Wizards neu definieren. Für die nicht löschbaren speziellen Standard-Rufnummern können Sie die vorbelegten Werte ändern.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie auf **Bearbeiten**, um den Wizard **Basisinstallation** zu starten.

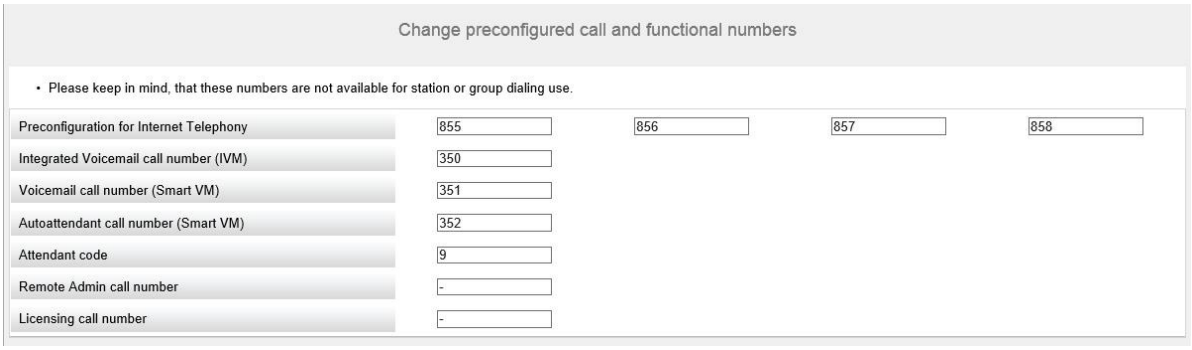
3) Klicken Sie auf **Weiter**.

> ***INFO:*** Eine Übersicht über die aktuell konfigurierten Rufnummern können Sie sich anzeigen lassen, indem Sie das Optionsfeld **Teilnehmerkonfiguration anzeigen** aktivieren und auf **Funktion ausführen** klicken.

4) Aktivieren Sie das Optionsfeld **Alle Rufnummern löschen**.

5) Aktivieren Sie in der Sicherheitsabfrage das Kontrollkästchen **Alle Rufnummern löschen**.

6) Klicken Sie auf **Funktion ausführen**.



7) Ändern Sie bei Bedarf in den Feldern die vorbelegten Werte der speziellen Standard-Rufnummern.

8) Klicken Sie auf **OK**. Die Rufnummern werden gelöscht und eventuelle Änderungen an den speziellen Standard-Rufnummern durchgeführt.

9) Klicken Sie auf **Abbrechen**, um den Wizard **Basisinstallation** zu beenden.

10.1.2.2 Wie Sie spezielle Standard-Rufnummern ändern

Sie können die für spezielle Funktionen vordefinierten Rufnummern ändern.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

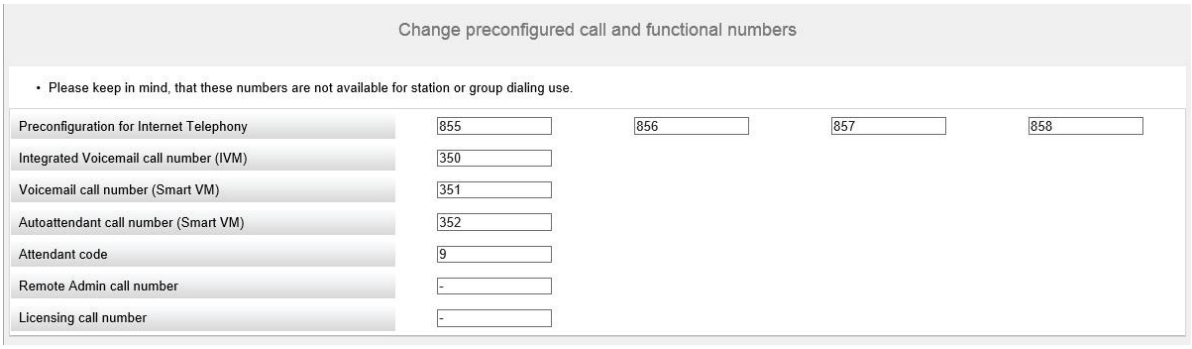
2) Klicken Sie auf **Bearbeiten**, um den Wizard **Basisinstallation** zu starten.

3) Klicken Sie auf **Weiter**.

> ***INFO:*** Eine Übersicht über die aktuell konfigurierten Rufnummern können Sie sich anzeigen lassen, indem Sie das Optionsfeld **Teilnehmerkonfiguration anzeigen** aktivieren und auf **Funktion ausführen** klicken.

4) Aktivieren Sie das Optionsfeld **Vorkonfigurierte Rufnummern ändern**.

5) Klicken Sie auf **Funktion ausführen**.



6) Geben Sie in den Feldern die gewünschten Rufnummern und Kennzahlen ein und klicken Sie auf **OK**. Die neuen Rufnummern und Kennzahlen sind gespeichert.

> ***INFO:*** Die hier konfigurierten Rufnummern können nicht als Teilnehmerrufnummern, Durchwahlrufnummern oder Gruppenrufnummern vergeben werden.

7) Klicken Sie auf **Abbrechen**, um den Wizard **Basisinstallation** zu beenden.

10.1.2.3 Wie Sie Rufnummern und Teilnehmerdaten importieren

Über eine XML-Datei können Sie vorab definierte Teilnehmerdaten importieren.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.
- Eine XML-Datei im UTF-8-Format mit den eingetragenen Daten liegt vor. Eine XML-Vorlage finden Sie unter **Service-Center > Dokumente > CSV-Vorlagen**.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie auf **Bearbeiten**, um den Wizard **Basisinstallation** zu starten.

3) Klicken Sie auf **Weiter**.

> ***INFO:*** Eine Übersicht über die aktuell konfigurierten Rufnummern können Sie sich anzeigen lassen, indem Sie das Optionsfeld **Teilnehmerkonfiguration anzeigen** aktivieren und auf **Funktion ausführen** klicken.

4) Aktivieren Sie das Optionsfeld **XML-Datei mit Teilnehmerdaten importieren**.

5) Klicken Sie auf **Funktion ausführen**.

6) Wählen Sie mit **Durchsuchen** die gewünschte XML-Datei aus und klicken sie auf **Öffnen**.

7) Klicken Sie anschließend auf **OK**. Die Teilnehmerdaten werden importiert.

8) Klicken Sie auf **Abbrechen**, um den Wizard **Basisinstallation** zu beenden.

10.2 Anforderungen an die LAN-Telefonie

Unter LAN-Telefonie versteht man das Kommunizieren von IP-Teilnehmern innerhalb des internen Netzes (LAN). Um die Qualität der Sprachübertragung bei der LAN-Telefonie sicherzustellen, müssen die verwendeten IP-Netze und das Kommunikationssystem bestimmte Anforderungen erfüllen. Die Sprachqualität und die Zuverlässigkeit der Sprachkommunikation hängt hierbei von der eingesetzten Netzwerktechnik ab.

Um eine verlustfreie Übertragung und eine gute Sprachqualität zu gewährleisten, werden die Sprachsignale mit Hilfe von Audio-Codecs digitalisiert und mit speziellen Verfahren (Quality of Service) so gekennzeichnet, dass die Sprachübertragung gegenüber der Datenübertragung vorrangig behandelt wird.

Anforderungen

- LAN mit mind. 100 Mbit/s und Full-Duplex
- Jede Komponente im IP-Netz muss an einem eigenen Port an einem Switch oder einem Router abgeschlossen sein; keinen HUB verwenden.

- Höchstens 50 ms Verzögerung in einer Richtung (One Way Delay); höchstens 150 ms Gesamtverzögerung
- Höchstens 3% Paketverlust; wird Fax/Modem über G.711 verwendet, darf der Paketverlust 0,05% nicht übersteigen.
- Höchstens 20 ms Jitter
- Unterstützung für Quality of Service (QoS): IEEE 802.p, DiffServ (RFC 2474) oder ToS (RFC 791)
- Höchstens 40% Netzwerkauslastung

10.2.1 Audio-Codecs

Als Audio-Codec bezeichnet man ein Programm, das Sprache in digitale Datenpakete (IP-Pakete) codiert und umgekehrt wieder decodiert. Abhängig vom verwendeten Audio-Codec können die Daten unterschiedlich stark komprimiert werden. Durch die Komprimierung wird bei der Übertragung des IP-Pakets weniger Bandbreite benötigt als ohne Komprimierung. Bei der Decodierung der Datenpakete kann es allerdings zu Einbußen der Sprachqualität und der Kontinuität der Wiedergabe kommen.

Damit die Daten nach dem Transport auch wieder korrekt in Sprache umgewandelt werden können, muss der Empfänger den gleichen Codec wie der Sender benutzen.

Unterstützte Audio-Codecs

Folgende Audio-Codecs werden unterstützt:

- G.729A, G.729AB: Sprachkodierung mit 8 Kbit/s - gute Sprachqualität.
- G.711 (A-law und µ-law): Sprachkodierung mit 56 oder 64 Kbit/s - sehr gute Sprachqualität. G.711 wird auch im Festnetzbereich (ISDN) eingesetzt.

Den Audio-Codecs können Prioritäten von 1 (hoch) bis 4 (niedrig) zugewiesen werden. Das Kommunikationssystem versucht automatisch, für jede Verbindung einen Audio-Codec mit einer möglichst hohen Priorität zu verwenden. Wird ein Audio-Codec mit geringer Sprachkomprimierung (guter Sprachqualität) verwendet, wird das Netz höher ausgelastet. Bei intensiver IP-Telefonie kann das bei einem durch Datentransfer bereits ausgelasteten Netz zu einer Verschlechterung der Sprachqualität führen.

Bei einigen Codecs kann das Kommunikationssystem eine Sprechpausenerkennung (VAD, Voice Activity Detection) aktivieren. Bei langen Sprechpausen kann somit die Last auf das Netz reduziert werden.

Für jeden Codec kann die Rahmengröße (Größe des IP-Pakets) von 10 bis zu 90 Millisekunden angegeben werden. Damit legen Sie die Abtastrate fest, mit der das Sprachsignal in IP-Pakete zerlegt wird. Ein höherer Wert (z. B. 90 ms) bedeutet einerseits ein besseres Verhältnis von Nutzdaten zum IP-Paket-Overhead, andererseits aber eine größere Verzögerung bei der Übertragung.

Es besteht die Möglichkeit, die ressourcen-hungrigen G.729-Codecs zu deaktivieren und nur die G.711-Codecs zu verwenden. Somit wird die Anzahl der

möglichen, parallel geführten Gespräche optimiert. Wird diese Funktion aktiviert, ist ein Neustart des Systems nötig.

10.2.1.1 Wie Sie Audio-Codec-Parameter konfigurieren

Voraussetzungen

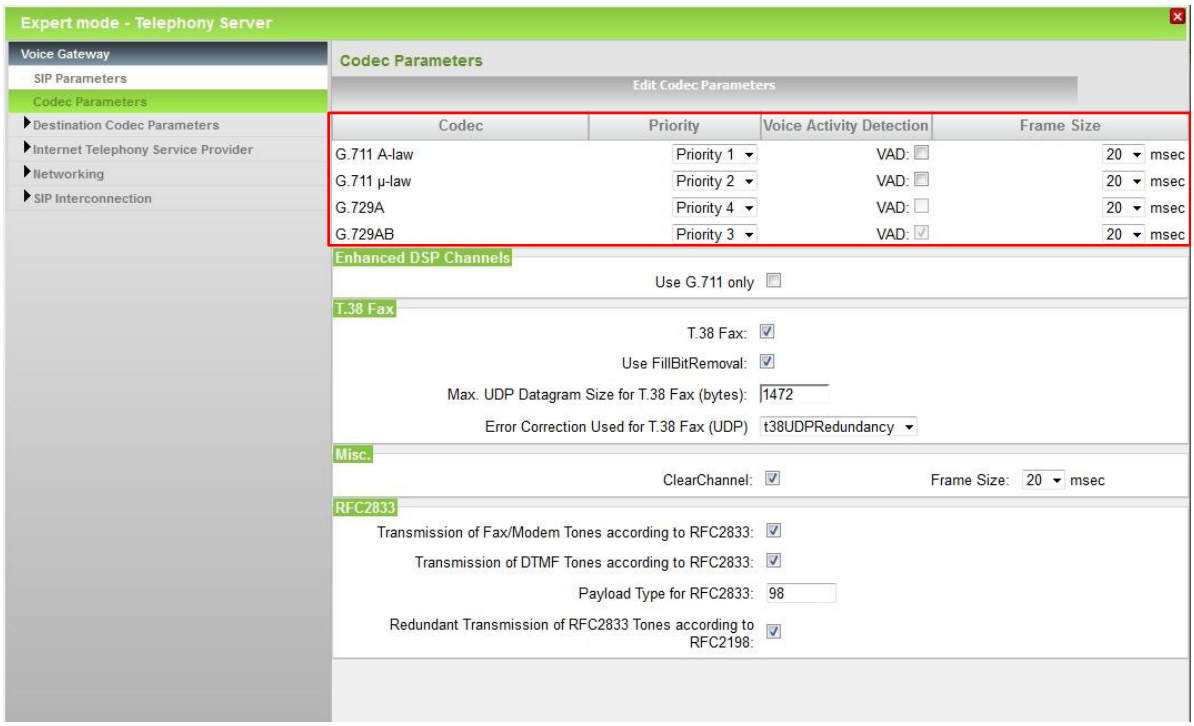
- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Sprachgateway**.

3) Klicken Sie im Menübaum auf **Codec-Parameter**.



4) Ordnen Sie den gewünschten Audio-Codecs über die Aufklappliste **Priorität** eine Priorität von 1 (hoch) bis 4 (niedrig) zu.

5) Aktivieren oder deaktivieren Sie bei den gewünschten Audio-Codecs das Optionsfeld **Sprechpausenerkennung (VAD)**.

6) Legen Sie bei den gewünschten Audio-Codecs im Feld **Rahmengröße** die Größe fest, in die der Audio-Codec die IP-Sprachpakete zerlegt.

7) Wenn Sie nur die beiden G.711-Audio-Codecs verwenden wollen, aktivieren Sie im Bereich **Erweiterte DSP-Kanäle** das Kontrollkästchen **Nur G.711 verwenden**.

8) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10.2.1.2 Wie Sie Audio-Codec-Parameter einem Ziel zuordnen

Voraussetzungen

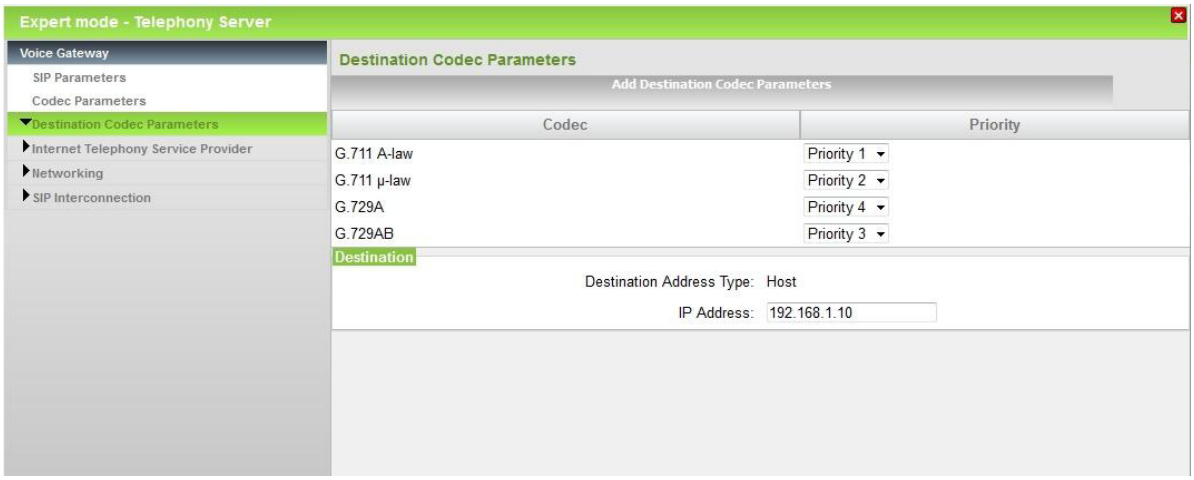
- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Sprachgateway**.

3) Klicken Sie im Menübaum auf **Ziel-Codec-Parameter**.



4) Ordnen Sie den gewünschten Audio-Codecs über die Aufklappliste **Priorität** eine Priorität von 1 (hoch) bis 4 (niedrig) zu.

5) Geben Sie unter **IP-Adresse** die IP-Adresse des Ziels ein, dem die zuvor eingestellten Prioritäten der Audio-Codec zugeordnet werden sollen (z. B. `192.168.1.10`).

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10.2.2 Übertragung von Tönen nach RFC2833

Die Übertragung von DTMF-Tönen und von Fax-/Modem-Tönen nach RFC2833 kann aktiviert oder deaktiviert werden.

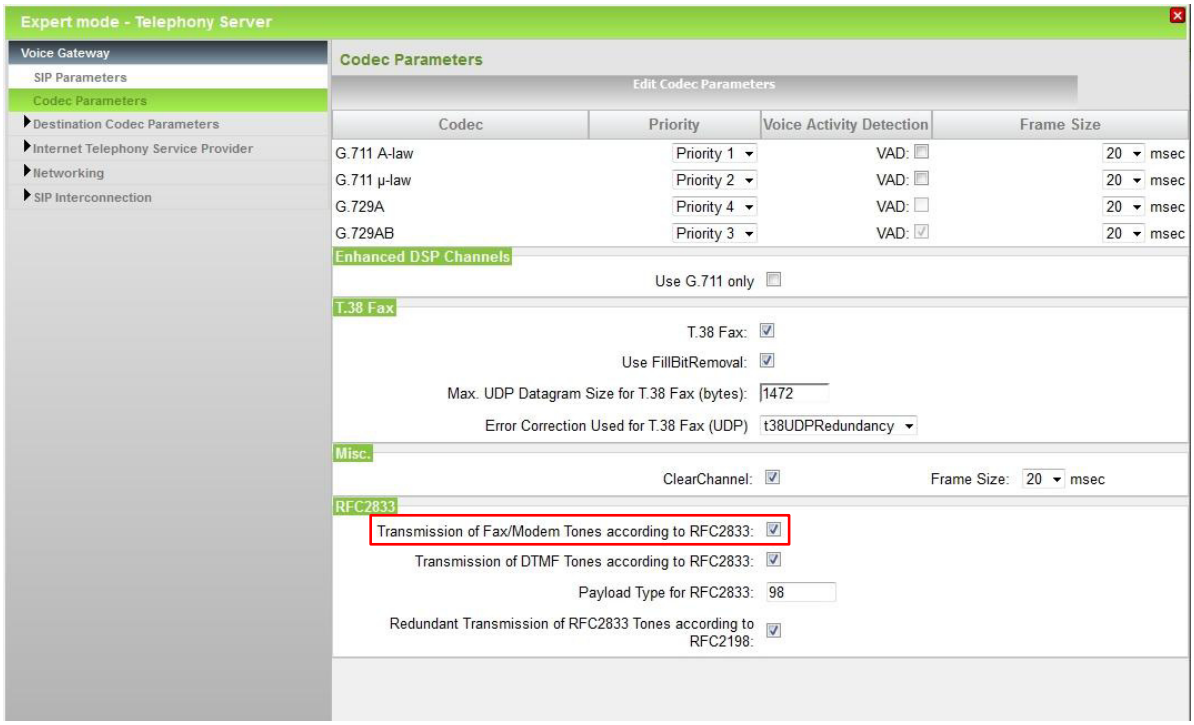
10.2.2.1 Wie Sie die Übertragung von Fax- und Modem-Tönen nach RFC2833 aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Sprachgateway**.
3) Klicken Sie im Menübaum auf **Codec-Parameter**.



4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie die Funktion aktivieren möchten, aktivieren Sie das Kontrollkästchen **Übertragung von Fax/Modem Tönen nach RFC2833**.
   - Wenn Sie die Funktion deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Übertragung von Fax/Modem Tönen nach RFC2833**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

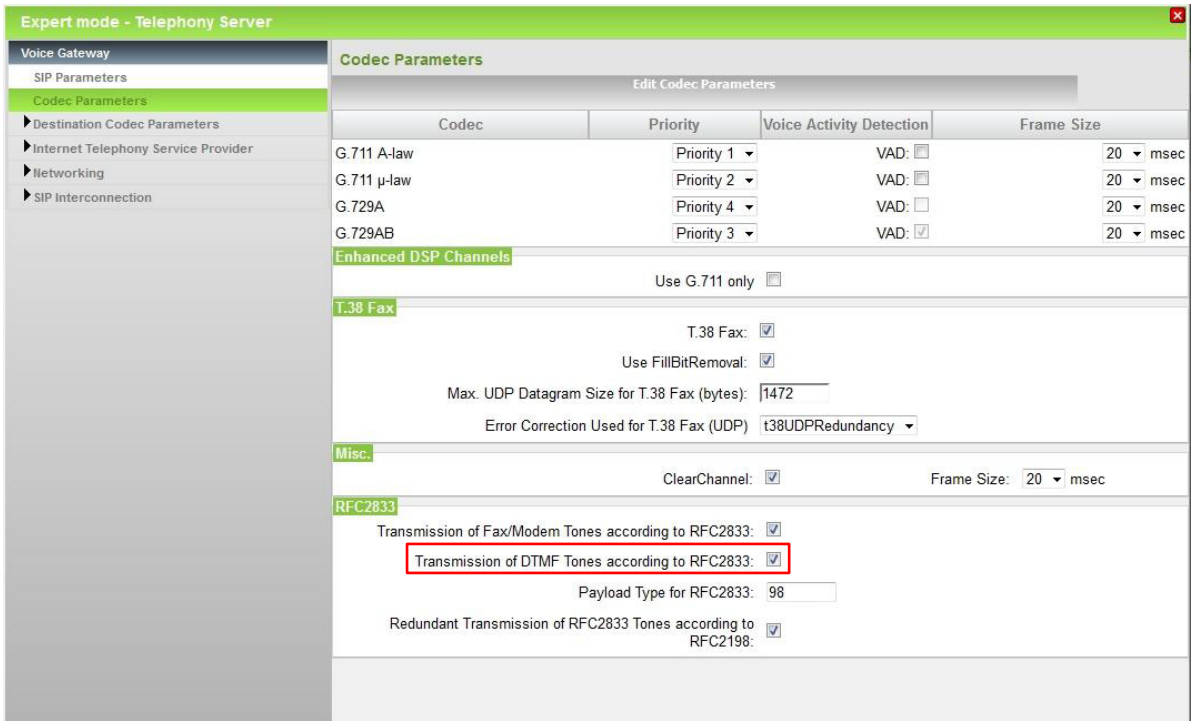
10.2.2.2 Wie Sie die Übertragung von DTMF-Tönen nach RFC2833 aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Sprachgateway**.
3) Klicken Sie im Menübaum auf **Codec-Parameter**.



4) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie die Funktion aktivieren möchten, aktivieren Sie das Kontrollkästchen **Übertragung von DTMF Tönen nach RFC2833**.
- Wenn Sie die Funktion deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Übertragung von DTMF Tönen nach RFC2833**.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10.2.3 Quality of Service

Quality of Service (QoS) umfasst unterschiedliche Verfahren, um die höchstmögliche Qualität und Verlustfreiheit bei der Übertragung von Datenpaketen (IP-Pakete) zu gewährleisten. Um bei der Sprachübertragung eine gute Sprachqualität zu erreichen, werden mit QoS im IP-Netz die IP-Sprachpakete vor den IP-Datenpaketen anderer Applikationen priorisiert.

Für die Priorisierung werden die IP-Pakete mit einer besonderen Markierung (Codepunkt) versehen. Die Priorisierungsinformation bewirkt eine Einstufung in unterschiedliche Klassen. Wenn die im IP-Netz vorhandenen Komponenten (z. B. Kommunikationssystem, SIP-Teilnehmer und Internet-Router) QoS unterstützen, können sie diesen Klassen unterschiedliche Bandbreite zuordnen und somit die IP-Sprachpakete bevorzugt transportieren.

Prioritätsklassen nach DiffServ

Für die Priorisierung nach dem DiffServ-Verfahren werden verschiedene Codepunkte für das Type of Service (ToS)- Feld definiert, um die Übertragung von IP-Paketen in unterschiedliche Klassen einteilen zu können.

- Codepunkt Expedited Forwarding (EF): Garantiert eine konstante Bandbreite. Für IP-Pakete, die mit diesem Codepunkt markiert sind, steht immer die gleiche Bandbreite zur Verfügung. Wird der festgelegte Wert erreicht, werden alle Pakete verworfen, die diese Bandbreite überschreiten.
- Codepunkt Assured Forwarding (AF): Garantiert eine minimale Bandbreite. IP-Pakete, die mit diesem Codepunkt markiert sind, haben eine niedrigere Priorität als EF und müssen sich die von EF nicht genutzte Bandbreite teilen. Wird der festgelegte Wert erreicht, werden alle IP-Pakete, die diese Bandbreite überschreiten würden, verworfen.
  Für AF sind vier Klassen reserviert: AF1x (niedrige Priorität) , AF2x, AF3x und AF4x (hohe Priorität), wobei x für einen von drei Dropping-Stufen steht: niedrig (1), mittel (2) und hoch (3). Bei niedrig werden Pakete lange zwischengespeichert, bei hoch werden Pakete früh verworfen, wenn sie nicht weitertransportiert werden können.
- Best Effort (BE): Unmarkierte IP-Pakete (Type of Service (ToS)-Feld=00) werden mit niedrigster Priorität behandelt.

Prioritätsklassen nach IP-Precedence

Neben dem DiffServ-Verfahren existieren verschiedene ältere Definitionen, die eine Priorisierung auf Basis des ToS-Feldes vornehmen. Für eine bestmögliche Anpassung des Kommunikationssystemes an die ggf. erforderlichen Einstellungen im Kundennetz können z. B. für IP-Precedence die Klassen 3 bis 7 (CS3-CS7) ausgewählt werden.

Individuelle Prioritätsklassen

Falls keine der voreingestellten Möglichkeiten im Kundennetz verwendet wird, kann der ToS-Wert auch direkt manuell eingestellt werden. Der eingestellte Wert wird dezimal 0-63 eingestellt und in die oberen 6 Bits des ToS-Bytes übernommen (z. B. 41 = 101-001-00 = 0xA4).

Tabelle der möglichen Prioritätsklassen

Prioritätsklasse	ToS-Wert Binär	ToS-Wert Hexadezimal
AF (Assured Forwarding)		
AF11	001-010-00	28
AF12	001-100-00	30
AF13	001-110-00	38
AF21	010-010-00	48
AF22	010-100-00	50
AF23	010-110-00	58
AF31	011-010-00	68

Prioritätsklasse	ToS-Wert Binär	ToS-Wert Hexadezimal
AF32	011-100-00	70
AF33	011-110-00	78
AF41	100-010-00	88
AF42	100-100-00	90
AF43	100-110-00	98
EF (Expedited Forwarding)		
EF	101-110-00	B8
Best Effort (BE)		
BE	000-000-00	00
CS (Class Selector)		
CS3	011-000-00	60
CS4	100-000-00	80
CS5	101-000-00	A0
CS6	110-000-00	C0
CS7	111-000-00	E0
Manuelle Eingabe	xxx-xxx-00	0-63 (dezimal)

10.2.3.1 Wie Sie Quality of Service konfigurieren

Voraussetzungen

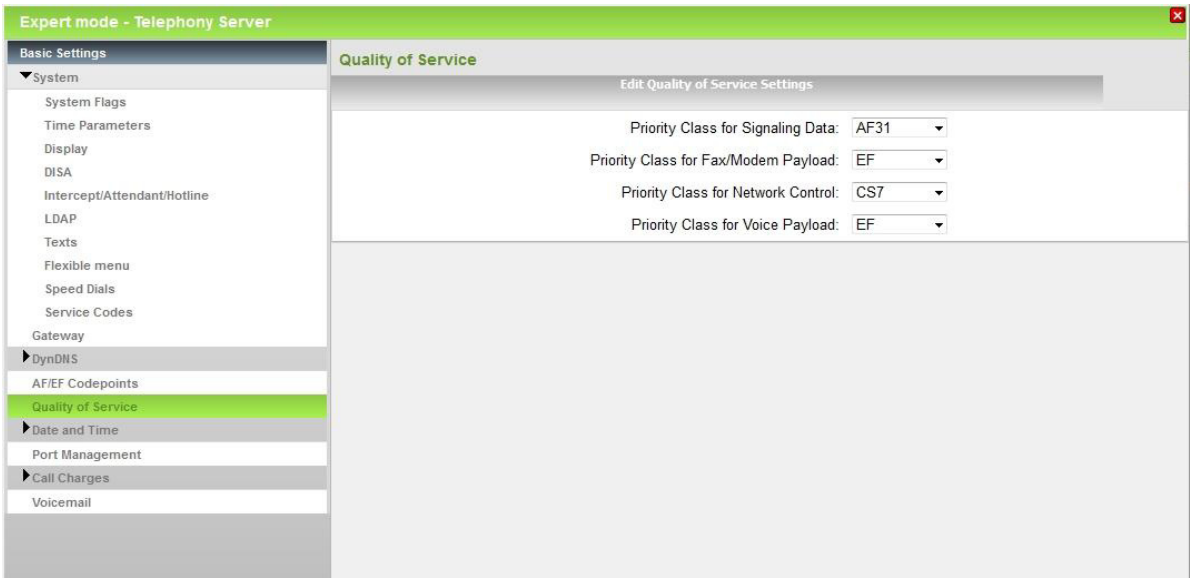
- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **Quality of Service**.



4) Wählen Sie aus der Aufklappliste **Prioritätsklasse für Signalisierungsdaten** die gewünschte Prioritätsklasse aus.

5) Wählen Sie aus der Aufklappliste **Prioritätsklasse für Fax/Modem-Payload** die gewünschte Prioritätsklasse aus.

6) Wählen Sie aus der Aufklappliste **Prioritätsklasse für Netzwerksteuerung** die gewünschte Prioritätsklasse aus.

7) Wählen Sie aus der Aufklappliste **Prioritätsklasse für Sprach-Payload** die gewünschte Prioritätsklasse aus.

8) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10.3 IP-Teilnehmer

IP-Teilnehmer sind über das LAN mit dem Kommunikationssystem verbunden. In der Regel ist ein IP-Teilnehmer ein LAN- oder WLAN-Telefon.

Folgende IP-Protokolle werden unterstützt:

- Herstellerabhängiges Protokoll des Kommunikationssystems
  Das Kommunikationssystem verwendet das auf Basis von H.323 weiterentwickelte CorNet-IP (CorNet-Internet-Protokoll) für die LAN-Telefonie innerhalb des internen Netzes. Mit CorNet-IP können alle Telefonleistungsmerkmale des Kommunikationssystems genutzt werden.
- SIP (Session Initiation Protocol)
  SIP wird üblicherweise bei der Internet-Telefonie eingesetzt, ist aber nicht darauf beschränkt. Es kann z. B. auch bei der Telefonie in internen Netzen verwendet werden. Mit SIP können aber nicht alle Telefonleistungsmerkmale des Kommunikationssystems genutzt werden.

Es gibt folgenden Typen von IP-Teilnehmern:

- **System-Client**: Ein System-Client ist ein IP-Teilnehmer, der über CorNet-IP alle Leistungsmerkmale des Kommunikationssystems nutzen kann. Das kann ein IP-Systemtelefon sein, wie z. B. ein OpenStage 60 HFA oder ein PC mit CTI-Software, wie OpenScape Personal Edition.
- **SIP-Client**: Ein SIP-Client ist ein IP-Teilnehmer, der das Protokoll SIP nutzt. Er kann über SIP nur einen eingeschränkten Leistungsumfang des Kommunikationssystems nutzen. Ein SIP-Client ist z. B. ein SIP-Telefon wie das OpenStage 15 S.
- **Deskshare User**: Ein Deskshare User ist ein IP-Teilnehmer, der sich auf einem anderen IP-Systemtelefon anmelden kann (Mobile Login) und dieses Telefon wie sein eigenes Telefon nutzen kann (inkl. Rufnummer).
- **RAS-User**: Einem RAS-User (Remote Access Service User) wird über den ISDN-Anschluss der Zugang zum IP-Netz gewährt. Dadurch kann das Kommunikationssystem ferngewartet werden.

Für jeden angeschlossenen IP-Teilnehmer ist eine Teilnehmer-Lizenz "IP User" nötig.

Zwei IP-Teilnehmer sind reserviert für den Online User und für den Remote-Zugang über ISDN. Diese IP-Teilnehmer benötigen keine Teilnehmer-Lizenz. Falls einer oder mehrere dieser drei reservierten IP-Teilnehmer nicht benötigt werden, können diese Teilnehmer über den Experten-Modus zu normalen IP-Teilnehmern umkonfiguriert werden. Dann werden für diese IP-Teilnehmer allerdings Teilnehmer-Lizenzen gebraucht.

Konfiguration der IP-Teilnehmer

Folgende Konfigurationen zu einem IP-Teilnehmer können durchgeführt werden:

- Konfiguration der Standard-Parameter mit dem Wizard IP-Endgeräte (siehe *Wie Sie IP-Teilnehmer konfigurieren*).
- Konfiguration aller Parameter (Standard-Parameter und erweiterte Parameter) über den Experten-Modus (siehe *Teilnehmer > Teilnehmer > IP Clients*).

10.4 SIP-Teilnehmer

SIP-Teilnehmer sind IP-Teilnehmer, die für die Kommunikation das Session Initiation Protocol (SIP) nutzen. Über dieses Protokoll kann der SIP-Teilnehmer einen eingeschränkten Leistungsumfang des Kommunikationssystems nutzen. SIP-Teilnehmer sind ebenso wie IP-Teilnehmer über das LAN mit dem Kommunikationssystem verbunden.

Ein SIP-Teilnehmer ist z. B. ein WLAN-Telefon oder ein LAN-Telefon wie das OpenStage 15 S.

Für jeden angeschlossenen SIP-Teilnehmer ist eine Teilnehmer-Lizenz "IP User" nötig.

SIP-Authentifizierung

Zur Sicherheit des internen Netzes ist es wichtig, dass sich die SIP-Teilnehmer am Kommunikationssystem mit den nachfolgend beschriebenen Werten authentifizieren. Diese Werte müssen im WBM des Kommunikationssystems für jeden SIP-Teilnehmer und auch an jedem SIP-Telefon selbst eingerichtet werden. Zum Schutz vor SIP-Attacken wird eine Authentifizierung dringend empfohlen!

- Kennwort
  Kennwort für die Authentifizierung: frei zu vergeben, mind. 8 Stellen - max. 20 Stellen. Das Kennwort sollte mind. einen Großbuchstaben, einen Kleinbuchstaben, eine Ziffer und ein Sonderzeichen enthalten. Für jeden SIP-Teilnehmer sollte ein eigenes Kennwort vergeben werden.
- SIP User ID / Benutzername
  Benutzername für die Authentifizierung: vorbelegt, kann bei Bedarf geändert werden, max. 20 Zeichen. Jeder SIP-Teilnehmer hat eine andere vorbelegte SIP User ID.
- Realm
  Zone oder Domäne für die Authentifizierung: vorbelegt, kann bei Bedarf geändert werden, max. 20 Zeichen. Der Realm ist für alle SIP-Teilnehmer mit dem gleichen Wert vorbelegt. Er kann bei Bedarf z. B. in den Host- oder Domänen-Namen des Kommunikationssystems geändert werden.

Konfiguration der SIP-Teilnehmer im Kommunikationssystem

Folgende Konfigurationen zu einem IP-Teilnehmer können im WBM des Kommunikationssystems durchgeführt werden:

- Konfiguration der Standard-Parameter mit dem Wizard IP-Endgeräte (siehe *Wie Sie SIP-Teilnehmer konfigurieren*).
- Konfiguration aller Parameter (Standard-Parameter und erweiterte Parameter) über den Experten-Modus (siehe *Teilnehmer > Teilnehmer > IP Clients*).

Konfiguration des SIP-Telefons

Die Daten für die Authentifizierung eines SIP-Teilnehmers am Kommunikationssystem müssen zusätzlich direkt am SIP-Telefon eingegeben werden.

Konfiguration der Authentifizierungsdaten am SIP-Telefon (siehe *Konfiguration der Authentifizierungsdaten am SIP-Telefon*).

Leistungsmerkmale, die mit SIP-Telefonen genutzt werden können

Folgende Leistungsmerkmale können mit SIP-Telefonen genutzt werden:

- kommende und gehende Anrufe mit Rufnummern- und Namensanzeige
- Halten, Makeln, Rückfrage
- Anruf übergeben vor und nach Melden
- Anruf übernehmen
- Anrufweiterleitung sofort, bei Besetzt und nach Zeit
- Dreierkonferenz
- Anruflisten, Nachrichtenlampe
- Ruhe vor dem Telefon, Ruf ablehnen, Ruf weiterleiten

- Anklopfen
- Mitgliedschaft in Gruppen (ohne Anzeige der Gruppenrufnummer)
- Unterschiedliche Rufe für Intern, Extern und Wiederanruf
- Briefkastenlampe - Message Waiting Indication
- DTMF-Nachwahl z B. für die Bedienung von Sprachboxen
- Nutzung der UC Clients
- Automatische SW-Updates (bei Nutzung des DLI)

> ***INFO:*** Der Einsatz mit Multichannel Contact Center ist nicht freigegeben.

Je nach Telefon können sich Einschränkungen der verfügbaren Funktionen ergeben siehe Wiki: `http://wiki.unify.com/wiki/SIP_devices_configuration_examples`

Folgende Leistungsmerkmale, die durch Kennzahlen mit * oder # aktiviert werden, können mit SIP-Telefonen genutzt werden:

- Services zurücksetzen: #0
- Sammelanschluss beitreten/verlassen: *85/#85
- Rufnummernunterdrückung (CLIR) ein/aus: *86/#86
- Kurzwahl: *7nnnn (nnnn = Kurzwahlnummer)
- Türöffner: *61

Leistungsmerkmale, die mit SIP-Telefonen und myPortal/myAttendant genutzt werden können

Für den Einsatz mit myPortal und myAttendant muss das verwendete SIP-Telefon folgende Voraussetzungen erfüllen:

- 3PCC gemäß RFC 3725 wird unterstützt.
- Das Leistungsmerkmal Anklopfen wird unterstützt.
- Der lokale Anklopfschutz ist deaktiviert.

Die vollständige Funktionalität der Leistungsmerkmale ist abhängig vom verwendeten SIP-Telefon und kann nicht gewährleistet werden. Der erfolgreiche Test der im folgenden aufgeführten Leistungsmerkmale erfolgte mit den OpenStage SIP Telefonen.

Verbindungs-/gesprächsorientierte Leistungsmerkmale:

- Anrufen
- Anruf weiterleiten
- Anruf übernehmen
- Anruf wiederaufnehmen
- Applikationsgesteuerte Konferenz
- Halten
- Makeln
- Rückfrage
- Trennen

- Übergabe

Telefonorientierte Leistungsmerkmale:

- Anrufschutz
- Anrufumleitung

10.5 UP0-Teilnehmer

Ein UP0-Teilnehmer nutzt für die Übertragung der digitalen Signale eine $U_{P0/E}$-Leitung. UP0-Teilnehmer werden über UP0-Schnittstellen an das Kommunikationssystem angeschlossen und sind Systemtelefone, wie z. B. ein OpenStage 60T. UP0-Teilnehmer können den kompletten Funktionsumfang des Kommunikationssystems nutzen.

Für einen UP0-Teilnehmer gibt es folgende Anschlussmöglichkeiten:

- OpenScape Business X1
  an die $U_{P0/E}$-Schnittstellen des Mainboards.
- OpenScape Business X3/X5
  an die $U_{P0/E}$-Schnittstellen des Mainboards oder bei vielen UP0-Teilnehmern an zusätzlich gesteckte $U_{P0/E}$-Baugruppen.
- OpenScape Business X8
  an zusätzlich gesteckte $U_{P0/E}$-Baugruppen.
- OpenScape Business S
  kein Anschluss möglich.

Für jeden angeschlossenen UP0-Teilnehmer ist eine Teilnehmer-Lizenz "TDM User" nötig. Auch Systemtelefone, die im Slave-Modus angeschlossen sind, benötigen eine Teilnehmerlizenz.

Konfiguration der UP0-Teilnehmer

Folgende Konfigurationen zu einem UP0-Teilnehmer können durchgeführt werden:

- Konfiguration der Standard-Parameter mit dem Wizard UP0-Endgeräte (siehe *Wie Sie UP0-Teilnehmer konfigurieren*).
- Konfiguration aller Parameter (Standard-Parameter und erweiterte Parameter) über den Experten-Modus (siehe *Teilnehmer > Teilnehmer > UP0 Teilnehmer*).

10.6 DECT-Teilnehmer

Ein DECT-Teilnehmer nutzt für die Übertragung der digitalen Signale eine Cordless-Basisstation. Ein DECT-Teilnehmer ist ein DECT-Telefon.

Für einen DECT-Teilnehmer gibt es folgende Anschlussmöglichkeiten:

- OpenScape Business X1/X3W/X3R/X5R
  Cordless-Basisstation an eine $U_{P0/E}$-Schnittstelle des Mainboards.

- OpenScape Business X5W
  Cordless-Basisstation an eine $U_{P0/E}$-Schnittstelle des Mainboards oder an eine SLC16N-Baugruppe.
- OpenScape Business X8
  Cordless-Basisstation an eine oder mehrere SLCN-Baugruppen.
- OpenScape Business S
  DECT IP-Basisstation im LAN

Der Anschluss einer Cordless-Basisstation nennt sich integrierte Cordless-Lösung. Damit stehen fast alle Funktionen des Kommunikationssystems zur Verfügung.

Die Integration einer DECT IP-Basisstation in das interne Netz nennt sich Cordless IP. Da in diesem Fall nur das SIP-Protokoll genutzt werden kann, stehen nicht alle Funktionen des Kommunikationssystems zur Verfügung.

Für jeden angeschlossenen DECT-Teilnehmer ist eine Teilnehmer-Lizenz "TDM User" nötig.

Für die Beschreibung und Konfiguration der integrierten Cordless-Lösung siehe *Integrierte Cordless-Lösung*.

Konfiguration der DECT-Teilnehmer

Folgende Konfigurationen zu einem DECT-Teilnehmer können durchgeführt werden:

- Konfiguration der Standard-Parameter mit dem Wizard DECT-Endgeräte (siehe *Wie Sie DECT-Teilnehmer konfigurieren*).
- Konfiguration aller Parameter (Standard-Parameter und erweiterte Parameter) über den Experten-Modus (siehe *Teilnehmer > Teilnehmer > DECT-Teilnehmer > DECT Teilnehmer*).

DECT IP-Teilnehmer werden wie normale SIP-Teilnehmer konfiguriert.

10.7 ISDN-Teilnehmer

Ein ISDN-Teilnehmer nutzt für die Übertragung der digitalen Signale den S_0-Bus. Deshalb wird er auch oft S_0-Teilnehmer genannt. Mit dem Kommunikationssystem wird der ISDN-Teilnehmer über die S_0-Schnittstellen verbunden.

Für einen S_0-Teilnehmer gibt es folgende Anschlussmöglichkeiten:

- OpenScape Business X1
  an eine S_0-Schnittstelle des Mainboards.
- OpenScape Business X3/X5
  an eine S_0-Schnittstelle des Mainboards oder an eine S_0-Baugruppe.
- OpenScape Business X8
  an eine oder mehrere S_0-Baugruppen.
- OpenScape Business S
  an zusätzlich benötigte Gateways oder Adapter

Folgende ISDN-Teilnehmer können angeschlossen werden:

- ISDN-Telefon
- Fax Gruppe 4
- ISDN-Modem
- PC mit ISDN-Karte

Folgende Typen von ISDN-Teilnehmern können definiert werden:

- Standard: für ISDN-Telefon, Fax Gruppe 4, ISDN-Modem oder PC mit ISDN-Karte
- Fax: Voraussetzung für die Einrichtung der Taste "Info von Fax/Anrufbeantworter". Wird z. B. ein PC mit ISDN-Karte und Faxsoftware an den S_0-Bus angeschlossen und ihm der Typ "Fax" zugewiesen, kann auf jedem Endgerät eine Taste "Info von Fax/Anrufbeantworter" eingerichtet werden. Wenn diese Taste leuchtet, wird damit signalisiert, dass ein Fax empfangen wurde.
- Anrufbeantworter: Voraussetzung für die Übernahme eines Gespräches, wenn der Anrufbeantworter das Gespräch bereits angenommen hat. Wird z. B. ein Gigaset ISDN mit Anrufbeantworter angeschlossen und ihm der Typ "Anrufbeantworter" zugewiesen, kann man auf jedem Endgerät ein Gespräch übernehmen, das der Anrufbeantworter bereits angenommen hat. Dazu muss am Endgerät eine Taste mit der internen Rufnummer des Gigasets programmiert werden.

Für jeden angeschlossenen ISDN-Teilnehmer ist eine Teilnehmer-Lizenz "TDM User" nötig.

Anschluss von ISDN-Teilnehmern an die S_0-Schnittstelle

Um ISDN-Teilnehmer an das Kommunikationssystem anschließen zu können, muss mindestens eine der S_0-Schnittstellen, die für den ISDN-Teilnehmeranschluss oder den ISDN-Anlagenanschluss verwendet werden, als interner S_0-Bus (S_0-Euro-Bus) konfiguriert werden.

INFO: Falls bei einem ISDN-Mehrgeräteanschluss mehrere ISDN-Teilnehmer an einer S_0-Schnittstelle angeschlossen werden (bis zu 8 ISDN-Teilnehmer möglich), muss jedem einzelnen ISDN-Teilnehmer eine eindeutige MSN zugeordnet werden. Diese Zuordnung ist im Konfigurationsmenü des ISDN-Teilnehmers durchzuführen.

Konfiguration der ISDN-Teilnehmer

Folgende Konfigurationen zu einem ISDN-Teilnehmer können durchgeführt werden:

- Konfiguration der Standard-Parameter mit dem Wizard ISDN-Endgeräte (siehe *Wie Sie ISDN-Teilnehmer konfigurieren*).
- Konfiguration aller Parameter (Standard-Parameter und erweiterte Parameter über den Experten-Modus (siehe *Teilnehmer > Teilnehmer > ISDN Teilnehmer*).

Nur eingerichtete Nummern für MSN zulassen

Der Administrator kann festlegen, dass weitere MSNs an einem S0-Bus nur für dort bereits vorhandene interne Rufnummern einrichtbar sind. In diesem Fall kann ein Teilnehmer nicht unberechtigt eine MSN hinzufügen, indem er den S0-Bus mit einer weiteren MSN gehend belegt und das Kommunikationssystem dem S0-Bus daraufhin eine freie interne Rufnummer für diese MSN zuordnet.

Umstecken am Bus

Das Kommunikationssystem unterstützt das Parken eines Gesprächs am S_0-Bus mit anschließendem Ausstecken und Anschließen des Endgeräts an einer anderen Stelle, um das Gespräch dann wieder aufzunehmen – Umstecken am Bus (Terminal Portability TP). Der geparkte Teilnehmer erhält eine Displaymeldung über den Umsteckvorgang. Für den gesamten Vorgang stehen drei Minuten zur Verfügung.

Für Dienste wie Telefax, Teletex oder Datenübermittlung wird das Leistungsmerkmal nicht unterstützt.

10.7.1 Wie Sie die S_0-Schnittstelle für ISDN-Teilnehmer konfigurieren

Mit dem Wizard **Amtsleitung ISDN / Analog / ITSP** können Sie eine oder mehrere S_0-Schnittstellen so konfigurieren, dass ISDN-Telefone daran angeschlossen werden können.

Voraussetzungen

- Es sind eine oder mehrere freie S_0-Schnittstellen vorhanden.
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

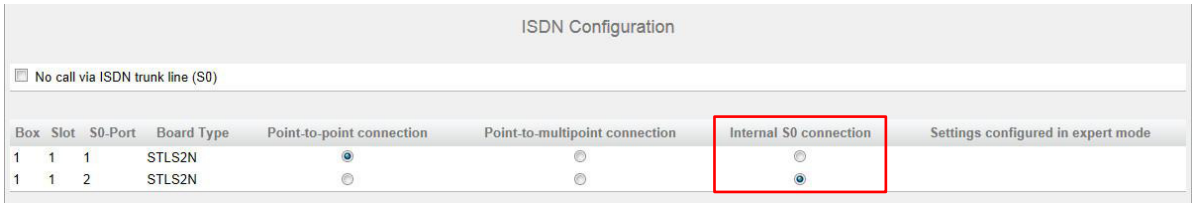
Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Zentrale Telefonie**.

3) Klicken Sie bei dem Wizard **Amtsleitung ISDN / Analog / ITSP** auf **Bearbeiten**.

4) Klicken Sie auf **OK & Weiter**. Es werden Ihnen die vorhandenen S_0-Schnittstellen (S_0-Ports) angezeigt.



5) Lassen Sie das Kontrollkästchen **Keine Telefonie über ISDN-Amtsleitung (S0)** so wie eingestellt.

6) Aktivieren Sie bei den gewünschten S_0-Schnittstellen das Optionsfeld **interner S0-Anschluss**.

> ***INFO:*** Diese S_0-Schnittstellen können Sie nicht mehr für den ISDN-Amtszugang nutzen.

7) Klicken Sie so oft auf **OK & Weiter**, bis Sie die Meldung erhalten, dass die Änderung des Leistungsmerkmals abgeschlossen ist.

8) Klicken Sie auf **Beenden**.

10.7.2 Wie Sie nur eingerichtete Nummern für MSN zulassen

Voraussetzungen

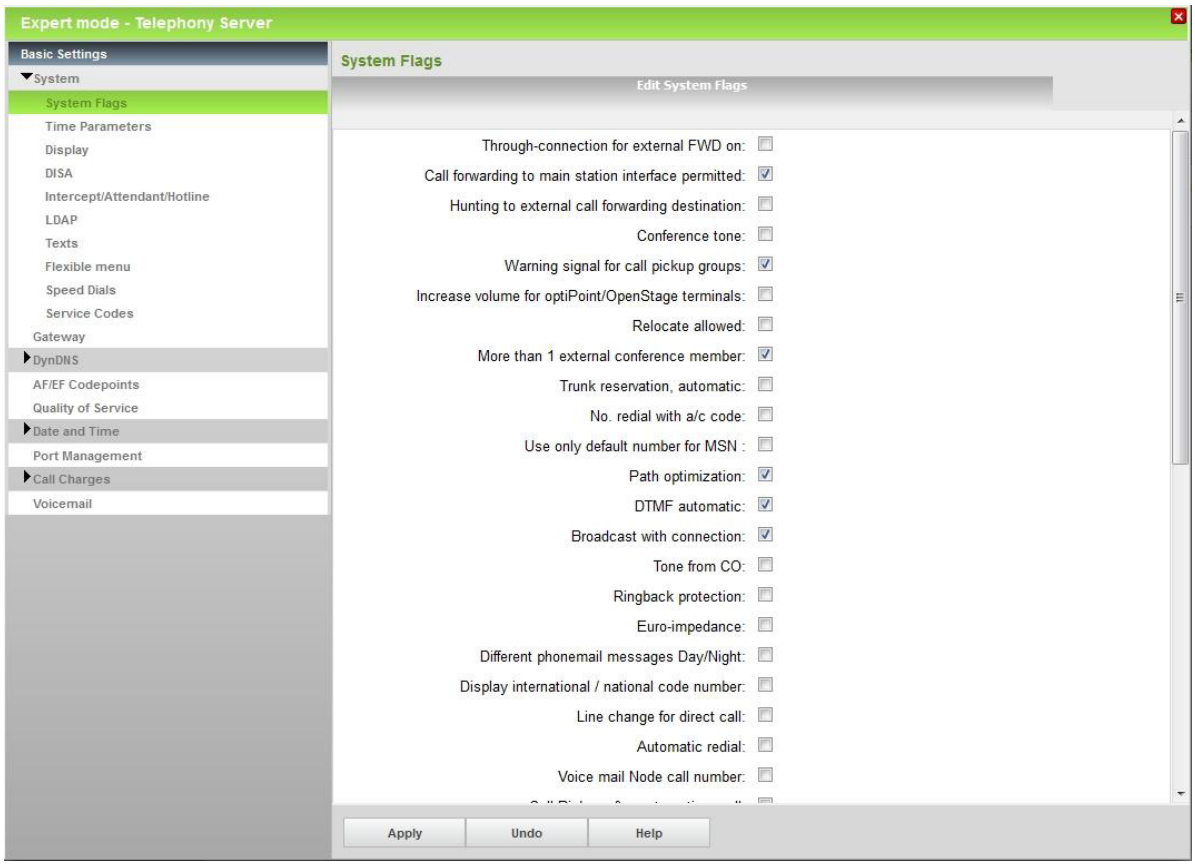
- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **Grundeinstellungen > System > System Flags**.



4) Wenn Sie nur eingerichtete Nummern für MSNs zulassen möchten, aktivieren Sie das Kontrollkästchen **Nur eingerichtete Nummer für MSN benutzen**.

5) Wenn Sie nicht nur eingerichtete Nummern für MSNs zulassen möchten, deaktivieren Sie das Kontrollkästchen **Nur eingerichtete Nummer für MSN benutzen**.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10.8 Analoge Teilnehmer

Ein analoger Teilnehmer (a/b-Teilnehmer) nutzt für die Übertragung der analogen Signale eine zweiadrige a/b-Leitung. Mit dem Kommunikationssystem wird der analoge Teilnehmer über die a/b-Anschlüsse verbunden.

Für einen analogen Teilnehmer gibt es folgende Anschlussmöglichkeiten:

- OpenScape Business X1
  an eine analoge Schnittstelle des Mainboards.
- OpenScape Business X3/X5
  an eine analoge Schnittstelle des Mainboards oder an eine analoge Baugruppe.
- OpenScape Business X8
  an eine oder mehrere analoge Baugruppen.

- OpenScape Business S
  an zusätzlich benötigte Gateways oder Adapter

Folgende analoge Teilnehmer können angeschlossen werden:

- Analoges Telefon
- Analoges Fax (Gruppe 3)
- Anrufbeantworter
- Modem ab 9600 bit/s
- Türsprechstelle
- Lautsprecher

Folgende Typen von analogen Teilnehmern können definiert werden:

- Standard: für analoges Telefon, Fax Gruppe 3, Anrufbeantworter oder Lautsprecher
- Fax: Voraussetzung für die Einrichtung der Taste "Info von Fax/Anrufbeantworter". Wird z. B. ein Fax Gruppe 3 angeschlossen und ihm der Typ "Fax" zugewiesen, kann auf jedem Endgerät eine Taste "Info von Fax/Anrufbeantworter" eingerichtet werden. Wenn diese Taste leuchtet, wird damit signalisiert, dass ein Fax empfangen wurde.
- Anrufbeantworter: Voraussetzung für die Übernahme eines Gespräches, wenn der Anrufbeantworter das Gespräch bereits angenommen hat. Wird z. B. ein Gigaset mit Anrufbeantworter angeschlossen und ihm der Typ "Anrufbeantworter" zugewiesen, kann man auf jedem Endgerät ein Gespräch übernehmen, das der Anrufbeantworter bereits angenommen hat. Dazu muss am Endgerät eine Taste mit der internen Rufnummer des Gigasets programmiert werden.
- Modem: Analoge Modems mit einer festen Geschwindigkeit von 56 kbit/s oder höher werden nicht unterstützt, da Geschwindigkeiten von 56 kbit/s oder höher nicht verarbeitet werden können.

Für jeden angeschlossenen analogen Teilnehmer ist eine Teilnehmer-Lizenz "TDM User" nötig.

Erreichbarkeit eines analogen Faxgeräts im System mit bisheriger Faxnummer

Da die Umleitung eines analogen Faxgerätes auf eine Faxnummer im System nicht möglich ist, besteht folgende Umgehungslösung: Die bisherige Faxnummer wird im System konfiguriert und erhält die ankommenden Faxnachrichten. Für das analoge Faxgerät wird ein Port konfiguriert mit der bisherigen Nummer als CLIP. Einstellbare CLIP muss aktiviert sein. Faxnachrichten nach extern zeigen die bisherige Nummer als Absender, interne Empfänger sehen die interne Nummer des Faxgerätes.

Konfiguration der analogen Teilnehmer

Folgende Konfigurationen zu einem analogen Teilnehmer können durchgeführt werden:

- Konfiguration der Standard-Parameter mit dem Wizard Analog-Endgeräte (siehe *Wie Sie analoge Teilnehmer konfigurieren*).

- Konfiguration aller Parameter (Standard-Parameter und erweiterte Parameter über den Experten-Modus (siehe *Teilnehmer > Teilnehmer > Analoge Teilnehmer*).

10.9 Virtuelle Teilnehmer

Virtuelle Teilnehmer verhalten sich wie reale Teilnehmer, ihnen sind aber keine physikalischen Endgeräte zugeordnet.

Virtuelle Teilnehmer werden z. B. für die Mobiltelefon-Integration und für die Rufweiterschaltung benötigt. Diese sind wie reale Teilnehmer zu konfigurieren, um z. B. für die Signalisierung von Anrufen verwendet zu werden.

Konfiguration der virtuellen Teilnehmer

Die Konfiguration der Parameter eines virtuellen Teilnehmers wird mit dem Experten-Modus durchgeführt (siehe *Teilnehmer > Teilnehmer > Virtuelle Teilnehmer*).

10.10 Tastenprogrammierung

Jedes Systemtelefon ist mit einer bestimmten Anzahl an Funktionstasten ausgestattet. Einige dieser Funktionstasten sind standardmäßig mit Funktionen vorbelegt. Diese Vorbelegung kann geändert und die restlichen nicht vorbelegten Funktionstasten können mit Funktionen programmiert werden.

Für die Tastenprogrammierung haben Sie folgende Möglichkeiten:

- Tastenprogrammierung über WBM
  Im WBM können über den Wizard **Tastenprogrammierung** die Tasten der angeschlossenen Systemtelefone programmiert werden.
  Über diesen Wizard kann auch für einen Teilnehmer eine Tastenbelegung programmiert werden, obwohl für diesen Teilnehmer noch kein Systemtelefon angeschlossen ist.
- Tastenprogrammierung über die UC Clients
  Nutzer der UC Clients **myPortal Smart**, **myPortal for Desktop**, **myPortal for Outlook** und **myAttendant** können die Tasten des Systemtelefons auch über die UC Clients programmieren (siehe Bedienungsanleitung der UC Clients).
- Tastenprogrammierung direkt am Systemtelefon
  Bei Systemtelefonen mit Display können bestimmte Funktionstasten auch direkt am Systemtelefon programmiert werden.

Mehrfachbelegung der Funktionstasten

Die Funktionstasten der Systemtelefone können zweifach belegt werden, nämlich auf der 1. Ebene und auf der 2. Ebene. Die 1.Ebene kann mit allen angebotenen Funktionen belegt werden. Die 2. Ebene kann mit externen Rufnummern belegt werden. Um die 2. Ebene verwenden zu können, muss am Systemtelefon die

Ebenenumschaltetaste (Shift-key) eingerichtet sein. Die LEDs der Funktionstasten gehört dabei immer zur 1. Ebene.

10.10.1 Wie Sie die Funktionstasten der Systemtelefone programmieren

Mit dem Wizard **Tastenprogrammierung** können Sie die Funktionstasten der Systemtelefone konfigurieren.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Endgeräte / Teilnehmer**.

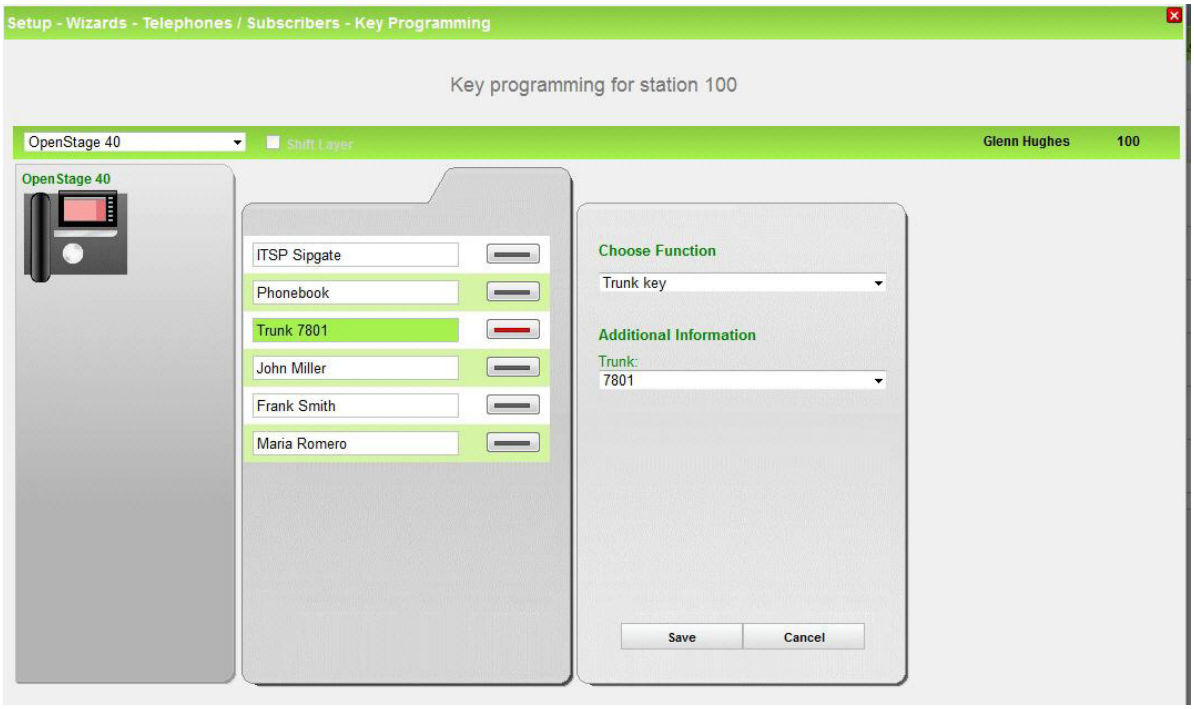
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Tastenprogrammierung** zu starten. Es wird die Liste aller Teilnehmer angezeigt.

4) Klicken Sie in der Zeile des gewünschten Teilnehmers auf **Bearbeiten**.

5) Ordnen Sie dem Teilnehmer das Systemtelefon zu:

- Ist für den Teilnehmer bereits ein Systemtelefon angeschlossen, wird Ihnen eine vereinfachte Darstellung des Systemtelefons angezeigt.
- Ist für den Teilnehmer noch kein Systemtelefon angeschlossen, wählen Sie in der Aufklappliste das anzuschließende Systemtelefon aus. Es wird Ihnen eine vereinfachte Darstellung des ausgewählten Systemtelefons angezeigt.

6) Klicken Sie in der vereinfachten Darstellung des Systemtelefons auf das gewünschte Tastenfeld. Es werden Ihnen die Funktionstasten des ausgewählten Tastenfelds angezeigt mit den momentan belegten Funktionen.



7) Belegen Sie die Funktionstasten:

a) Klicken Sie bei der zu belegenden Funktionstaste auf das Tastensymbol. Es wird Ihnen eine Aufklappliste mit den möglichen Funktionen angezeigt.

b) Wählen Sie in der Aufklappliste **Funktion auswählen** eine der angebotenen Möglichkeiten aus.

c) Einige Funktionen erfordern Zusatzinformationen. Wählen Sie diese falls erforderlich aus bzw. geben Sie die erforderlichen Daten ein.

d) Klicken Sie auf **Speichern**.

e) Ändern Sie im Feld **neue Beschriftung eingeben** bei Bedarf die Beschriftung der Funktionstaste.

INFO: Haben Sie ein Systemtelefon mit automatischer Tastenbeschriftung (z. B. OpenStage 60 HFA), wird dieser Text vom Systemtelefon übernommen.

---

f) Klicken Sie auf **Speichern**.

g) Wenn Sie weitere Funktionstasten belegen wollen, wiederholen Sie Schritt 7.

8) Haben Sie auf einer Funktionstaste die **Ebenenumschaltung** eingerichtet, aktivieren Sie das Kontrollkästchen **Ebenenumschaltung**. Belegen Sie die zweite Ebene der Funktionstasten mit den externen Rufnummern wie unter Schritt 7 beschrieben.

9) Klicken Sie auf **Tastenlayout übernehmen**.

10) Wenn Sie die soeben definierte Tastenbelegung für mehrere oder alle Systemtelefone übernehmen wollen, aktivieren Sie bei den gewünschten Systemtelefonen das Kontrollkästchen, klicken Sie anschließend auf **Übernehmen**, auf **OK** und auf **OK & Weiter**.

11) Wenn Sie die soeben definierte Tastenbelegung nur für das ausgewählte Systemtelefon übernehmen wollen, klicken Sie zur Sicherheit auf **Alle Teilnehmer deselektieren** und anschließend auf **OK & Weiter**.

12) Klicken Sie auf **Weiter** und anschließend auf **Beenden**.

10.11 Teilnehmer-Profile

In Profilen werden die Werte und Eigenschaften von Teilnehmern abgespeichert. Einem Profil können mehrere Mitglieder zugeordnet werden. Für alle Mitglieder dieses Profils gelten die gleichen Werte und Eigenschaften.

Teilnehmer-Profile können Teilnehmern mit Systemtelefonen zugeordnet werden. Es können bis zu 20 Teilnehmer-Profile angelegt werden. Die Teilnehmer-Profile können einzeln oder alle zusammen exportiert und importiert werden. Die Dateien sind vom Typ `xml`.

Jeder Teilnehmer kann Mitglied von genau einem Profil sein. Werden die Werte und Eigenschaften eines Teilnehmers, der Mitglied eines Profils ist, direkt - also nicht über das Profil - geändert, so wird der Teilnehmer aus dem Profil gelöscht.

10.12 Konfiguration der Teilnehmer

Für die Teilnehmer können bestimmte Werte (z. B. Rufnummer, Name und Durchwahlnummer) und Eigenschaften (z. B. Art der Rufsignalisierung) definiert werden.

Die Konfiguration der Teilnehmer ist unterteilt in eine Standard-Konfiguration und eine erweiterte Konfiguration. Die Standard-Einstellungen können über Wizards mit dem Profil "Advanced" konfiguriert werden. Die erweiterten Einstellungen können nur über den Experten-Modus mit dem Profil "Expert" konfiguriert werden.

Die Standard-Einstellungen lassen sich für alle Teilnehmer einer Teilnehmerart (z. B. IP-Teilnehmer oder analoge Teilnehmer) komfortabel in einer Liste ändern.

Virtuelle Teilnehmer werden komplett über den Experten-Modus konfiguriert (sowohl die Standard-Einstellungen als auch die erweiterten Einstellungen).

Mit dem Profil "Basic" können die Teilnehmer zwar nicht konfiguriert werden, aber die Namen der Teilnehmer können geändert werden.

Für die am Kommunikationssystem angeschlossenen Teilnehmer sollte ein Rufnummernplan existieren. Rufnummern, Namen und Durchwahlnummern aller konfigurierten Teilnehmer können über den Experten-Modus unter **Teilnehmer > Durchwahl Rufnummern** angezeigt werden.

Durchwahlnummern, die nicht vom Service Provider zur Verfügung gestellt und nicht im System genutzt werden, sollten gelöscht werden, sonst kann es zu Konflikten mit MSN oder Internet-Telefonie-Teilnehmerrufnummern kommen. Durchwahlnummern, die von einem Internet-Telefonie-Service-Provider (ITSP) zur Verfügung gestellt werden, sind bei der Einrichtung des ITSP den Teilnehmern zuzuordnen (siehe *Konfiguration eines ITSP*).

> ***WICHTIG:*** Die Änderung einer Teilnehmerrufnummer setzt die für den Teilnehmer eventuell eingerichtete Smart VM (Voicemail) zurück. Alle persönlichen Sprachnachrichten, Begrüßungen und Ansagen gehen verloren und das Kennwort wird zurückgesetzt.

Standard-Einstellungen

Die Standard-Einstellungen sollten für jeden Teilnehmer kontrolliert und wenn nötig angepasst werden.

- **Rufnummer, Name, Durchwahlnummer**
  Standardmäßig ist jedem Teilnehmer eine Rufnummer zugeordnet (z. B. 101). Unter dieser Rufnummer ist der Teilnehmer intern erreichbar. Bei Systemtelefonen wird diese Rufnummer im eigenen Display und im Display des Kommunikationspartners angezeigt. Soll beim extern angerufenen Teilnehmer an Stelle der eigentlichen Rufnummer eine andere Rufnummer angezeigt werden, kann diese Rufnummer definiert werden.
  Jedem Teilnehmer kann zusätzlich eine Durchwahlnummer zugeordnet werden. Unter der Durchwahlnummer ist der Teilnehmer von extern direkt erreichbar. Der Teilnehmer kann z. B. intern über die Rufnummer 101 und extern über die Durchwahlnummer `3654321` (MSN bei Mehrgeräteanschluss) oder `<Anlagenrufnummer>-101` (bei Anlagenanschluss) erreicht werden. Bei der Erstinstallation kann im Falle eines Anlagenanschlusses festgelegt werden, ob als Durchwahlnummer automatisch die interne Rufnummer eingetragen werden soll. Die Durchwahlnummer kann sich aber auch von der Rufnummer unterscheiden. Falls Internet-Telefonie genutzt wird, kann zusätzlich eine Durchwahlnummer festgelegt werden, mit der der Teilnehmer über die Internet-Telefonie erreichbar ist. Diese Rufnummer wird vom Internet-Telefonie-Service-Provider zur Verfügung gestellt.
  Jedem Teilnehmer kann zusätzlich ein Name zugeordnet werden. Dieser Name erscheint beim Kommunikationspartner im Display (nur bei Systemtelefonen).
  Existiert ein Rufnummernplan, so sollten die Rufnummern, die Durchwahlnummern und die Namen der Teilnehmer anhand des Rufnummernplans angepasst werden.
- **Typ**
  Für jeden Teilnehmer kann der Teilnehmertyp ausgewählt werden. Ein IP-Teilnehmer kann z. B. vom Teilnehmertyp **System Client** oder **SIP Client** sein, ein analoger Teilnehmer kann ein analoges Telefon oder ein analoges Faxgerät sein und ein ISDN-Teilnehmer kann ein ISDN-Telefon oder ein ISDN-Fax sein.

- **Berechtigungsklassen**
  Einem Teilnehmer kann eine von 15 verschiedenen Berechtigungsklassen zugewiesen werden. Damit wird z. B. festgelegt, ob der Teilnehmer externe Gespräche annehmen und führen darf oder welche Rufnummern der Teilnehmer wählen darf und welche nicht (siehe *Berechtigungen (Wahlkontrolle)*).
- **Anrufübernahmegruppen**
  Jeder Teilnehmer kann einer Anrufübernahmegruppe zugeordnet werden.
- **Sprache, Rufsignalisierung**
  Die Sprache für die Menüsteuerung der angeschlossenen Systemtelefone kann einstellt werden.
  Der Klang des Ruftons eines externen und eines internen Anrufs kann ausgewählt werden.
- **Sprachbox (nur mit UC Smart)**
  Bei der UC-Lösung UC Smart kann man für jeden Teilnehmer eine Sprachbox einrichten und zwischen verschiedenen Begrüßungsansagen wählen. Für genauere Informationen zur Sprachbox siehe *Sprachbox / SmartVM (UC Smart)*
  Bei der UC-Lösung UC Suite wird jedem Teilnehmer automatisch eine Sprachbox zugewiesen. Somit fehlen in diesem Fall die Sprachbox-Einstellungen.

Erweiterte Einstellungen

Über den Experten-Modus können alle Einstellungen für alle Arten von Teilnehmern konfiguriert werden. Die erweiterten Einstellungen können für den Standard-Betrieb wie eingestellt belassen werden und müssen nur im Bedarfsfall angepasst werden. Informationen zu den erweiterten Einstellungen siehe *Teilnehmer*.

Verwandte Themen

- Berechtigungen (Wahlkontrolle)

10.12.1 Wie Sie IP-Teilnehmer konfigurieren

Mit dem Wizard **IP-Endgeräte** können Sie die IP-Teilnehmer (LAN-Telefone und WLAN-Telefone) konfigurieren.

Voraussetzungen

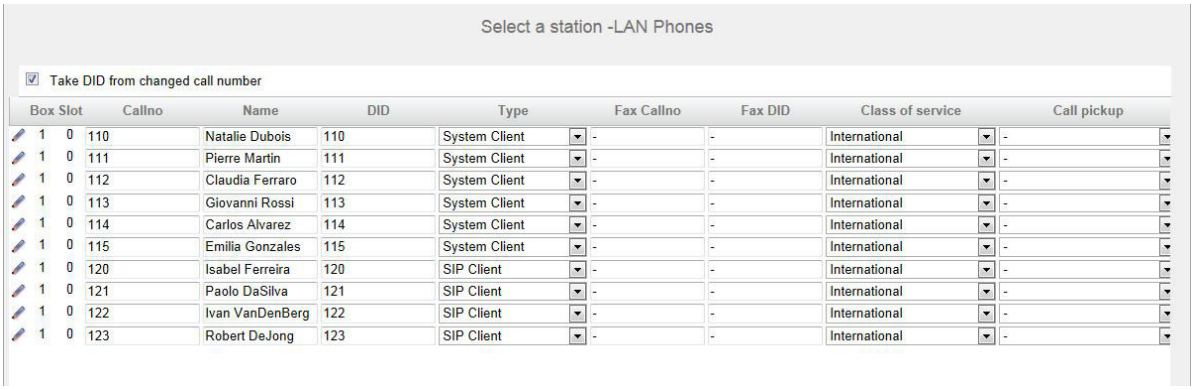
- Für den Betrieb von WLAN-Telefonen benötigen Sie ein funktionsfähiges Wireless LAN-Netzwerk.
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Endgeräte/Teilnehmer**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **IP-Endgeräte** zu starten. Es wird Ihnen eine Liste aller IP-Teilnehmer angezeigt.



4) Wenn der Teilnehmer automatisch als Durchwahlnummer die interne Rufnummer bekommen soll, aktivieren Sie das Optionsfeld **Durchwahl bei Eingabe der Rufnummer übernehmen**.

5) Wenn sich die Durchwahlnummer des Teilnehmers von seiner Rufnummer unterscheiden soll, geben Sie in der Zeile des gewünschten Teilnehmers unter **DuWa** eine Durchwahl-Nummer für den Teilnehmer ein:

- nur bei Anlagenanschluss:

  Klicken Sie in das gewünschte Feld und geben Sie über die Tastatur die Durchwahlnummer ein. Die Durchwahlnummer kann auch mit der internen Rufnummer identisch sein.

- nur bei Mehrgeräteanschluss:

  Wählen Sie in dem gewünschten Feld über die Aufklappliste eine MSN aus. Der Teilnehmer kann z. B. von intern über die interne Rufnummer 101 und von extern über die MSN 654321 erreicht werden.

- bei Anlagenanschluss und Mehrgeräteanschluss:

  Wählen Sie in dem gewünschten Feld über die Aufklappliste den Eintrag **xxx - änderbar** aus (xxx steht für die interne Rufnummer) und geben Sie über die Tastatur die Durchwahlnummer ein oder wählen Sie über die Aufklappliste eine MSN aus.

6) Wenn der Teilnehmer eine Internet-Telefonie-Teilnehmerrufnummer als Durchwahlnummer erhalten soll, lassen Sie das Optionsfeld **Durchwahl bei Eingabe der Rufnummer übernehmen** deaktiviert, wählen Sie aus der Liste neben diesem Optionsfeld den Internet-Telefonie-Service-Provider aus und wählen in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **DuWa** die Internet-Telefonie-Teilnehmerrufnummer aus.

7) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Rufnr** eine interne Rufnummer für den Teilnehmer ein. Sie können die vorbelegte Rufnummer verwenden oder eine andere, noch nicht belegte Rufnummer vergeben.

8) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Name** einen Namen in der Form `Nachname,Vorname` oder `Vorname Nachname` ein.

9) Wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Typ** den Typ des IP-Teilnehmers aus (z. B. **System Client** oder **Deskshare User**).

10) Wenn für den Teilnehmer eine Faxbox eingerichtet werden soll (nutzbar z. B. mit den UC Clients **myPortal for Desktop** oder **myPortal for Outlook**), gehen Sie folgendermaßen vor:

a) Geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax Rufnr** die gewünschte interne Fax-Rufnummer ein, unter der der Teilnehmer von intern Faxnachrichten empfangen kann.

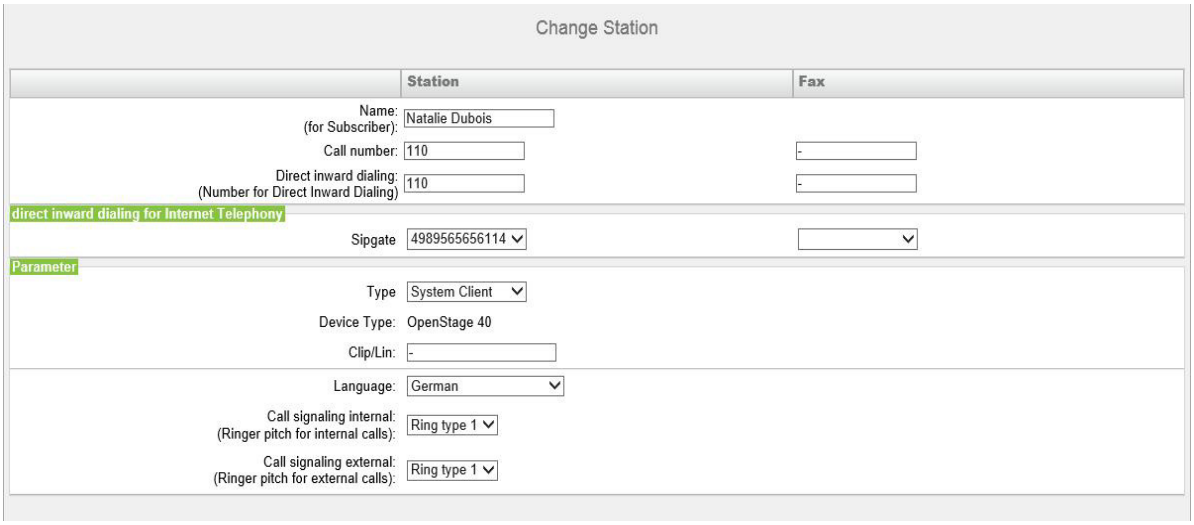
b) Wenn für die Faxbox eine Durchwahlnummer konfiguriert werden soll, geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax DuWa** die gewünschte externe Fax-Rufnummer ein, unter der der Teilnehmer von extern Faxnachrichten empfangen kann.

11) Wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Berechtigung** die gewünschte Berechtigungsgruppe aus.

12) Um den Teilnehmer in eine Anrufübernahmegruppe aufzunehmen, wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Anrufübernahme** eine Anrufübernahmegruppe aus.

13) Führen Sie bei Bedarf weitere Einstellungen durch:

a) Klicken Sie in der Zeile des gewünschten Teilnehmers auf das Stiftsymbol **Bearbeiten**.



b) Ordnen Sie im Bereich **Durchwahl für Internet-Telefonie** dem Teilnehmer und falls gewünscht seiner Faxbox jeweils eine Durchwahlnummer für die Internet-Telefonie zu. Wählen Sie dazu aus den Aufklapplisten des gewünschten ITSP die Durchwahlnummern aus. Für jeden aktiven ITSP wird Ihnen eine Aufklappliste für den Teilnehmer und eine Aufklappliste für seine Faxbox angezeigt.

INFO: Das Feld **Durchwahl für Internet-Telefonie** ist nicht sichtbar, wenn die Internet-Telefonie nicht eingerichtet oder kein Internet-Telefonie-Service-Provider aktiviert ist.

---

c) Geben Sie im Feld **Clip/Lin** eine Rufnummer ein (Durchwahlnummer oder MSN), die beim einem externen Anruf im Display des Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird.

INFO: Dieses Leistungsmerkmal muss vom Netzanbieter freigegeben sein.

---

d) Wählen Sie aus der Aufklappliste **Sprache** die Sprache für die Menüsteuerung des Telefons aus.

e) Weisen Sie aus der Aufklappliste **Rufsignalisierung intern** dem Teilnehmer eine von insgesamt acht möglichen akustischen Rufsignalisierungen für interne Anrufe zu. Dadurch sendet der Teilnehmer anderen internen Teilnehmern einen veränderten Rufton, durch den er von anderen Teilnehmern unterschieden werden kann (Standard: Rufart 1).

f) Weisen Sie aus der Aufklappliste **Rufsignalisierung extern** dem Teilnehmer eine von insgesamt drei möglichen akustischen Rufsignalisierungen für externe Anrufe zu (Standard: Rufart 1).

g) Nur bei UC Smart: Wählen Sie in der Aufklappliste **Mailboxtyp UC Smart** aus, ob der Teilnehmer eine Standardmailbox oder eine Vermittlungsmailbox (AutoAttendant) erhalten soll.

h) Nur bei UC Smart und Standardmailbox: Wenn ein Anrufer eine Nachricht auf der Sprachbox hinterlassen darf, aktivieren Sie das Kontrollkästchen **Aufnahme**.

i) Nur bei UC Smart: Wählen Sie aus der Aufklappliste **Begrüßung** eine Begrüßung aus.

j) Nur bei UC Smart: Wenn das Kennwort der Sprachbox zurückgesetzt werden soll, aktivieren Sie das Kontrollkästchen **Passwort Reset**.

INFO: Das Kontrollkästchen **Passwort Reset** muss bei einer Neueinrichtung einer Sprachbox nicht gesetzt sein. Es bewirkt das Rücksetzen des Kennworts der Sprachbox. Bei einer Neueinrichtung muss der Teilnehmer sowieso beim ersten Zugriff auf seine Sprachbox das Initial-Kennwort ändern.

---

k) Klicken Sie auf **OK & Weiter**.

14) Wenn Sie einen weiteren Teilnehmer einrichten möchten, wiederholen Sie die Schritte 5 bis 13.

15) Klicken Sie auf **OK & Weiter**. Sie sehen eine Liste aller eingerichteten IP-Teilnehmer. Bei Bedarf können Sie sich mit **Drucken** die Liste der IP-Teilnehmer ausdrucken.

16) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

10.12.2 Wie Sie SIP-Teilnehmer konfigurieren

Mit dem Wizard **IP-Endgeräte** können Sie die SIP-Teilnehmer (LAN-Telefone und WLAN-Telefone) konfigurieren.

Voraussetzungen

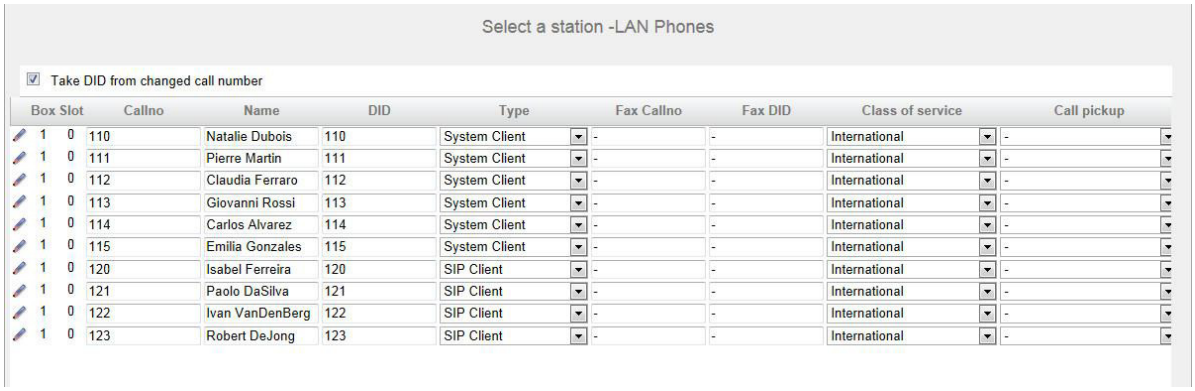
- Für den Betrieb von WLAN-Telefonen benötigen Sie ein funktionsfähiges Wireless LAN-Netzwerk.
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Endgeräte/Teilnehmer**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **IP-Endgeräte** zu starten. Es wird Ihnen eine Liste aller IP-Teilnehmer angezeigt. Diese Liste enthält auch alle SIP-Teilnehmer.



4) Wenn der Teilnehmer automatisch als Durchwahlnummer die interne Rufnummer bekommen soll, aktivieren Sie das Optionsfeld **Durchwahl bei Eingabe der Rufnummer übernehmen**.

5) Wenn sich die Durchwahlnummer des Teilnehmers von seiner Rufnummer unterscheiden soll, geben Sie in der Zeile des gewünschten Teilnehmers unter **DuWa** eine Durchwahl-Nummer für den Teilnehmer ein:

- nur bei Anlagenanschluss:

  Klicken Sie in das gewünschte Feld und geben Sie über die Tastatur die Durchwahlnummer ein. Die Durchwahlnummer kann auch mit der internen Rufnummer identisch sein.

- nur bei Mehrgeräteanschluss:

  Wählen Sie in dem gewünschten Feld über die Aufklappliste eine MSN aus. Der Teilnehmer kann z. B. von intern über die interne Rufnummer 101 und von extern über die MSN 654321 erreicht werden.

- bei Anlagenanschluss und Mehrgeräteanschluss:

  Wählen Sie in dem gewünschten Feld über die Aufklappliste den Eintrag **xxx - änderbar** aus (xxx steht für die interne Rufnummer) und geben Sie über die Tastatur die Durchwahlnummer ein oder wählen Sie über die Aufklappliste eine MSN aus.

6) Wenn der Teilnehmer eine Internet-Telefonie-Teilnehmerrufnummer als Durchwahlnummer erhalten soll, lassen Sie das Optionsfeld **Durchwahl bei Eingabe der Rufnummer übernehmen** deaktiviert, wählen Sie aus der Liste neben diesem Optionsfeld den Internet-Telefonie-Service-Provider aus und wählen in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **DuWa** die Internet-Telefonie-Teilnehmerrufnummer aus.

7) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Rufnr** eine interne Rufnummer für den Teilnehmer ein. Sie können die vorbelegte Rufnummer verwenden oder eine andere, noch nicht belegte Rufnummer vergeben.

8) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Name** einen Namen in der Form `Nachname,Vorname` oder `Vorname Nachname` ein.

9) Wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Typ** den Typ **SIP Client** aus.

10) Wenn für den Teilnehmer eine Faxbox eingerichtet werden soll (nutzbar z. B. mit den UC Clients **myPortal for Desktop** oder **myPortal for Outlook**), gehen Sie folgendermaßen vor:

a) Geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax Rufnr** die gewünschte interne Fax-Rufnummer ein, unter der der Teilnehmer von intern Faxnachrichten empfangen kann.

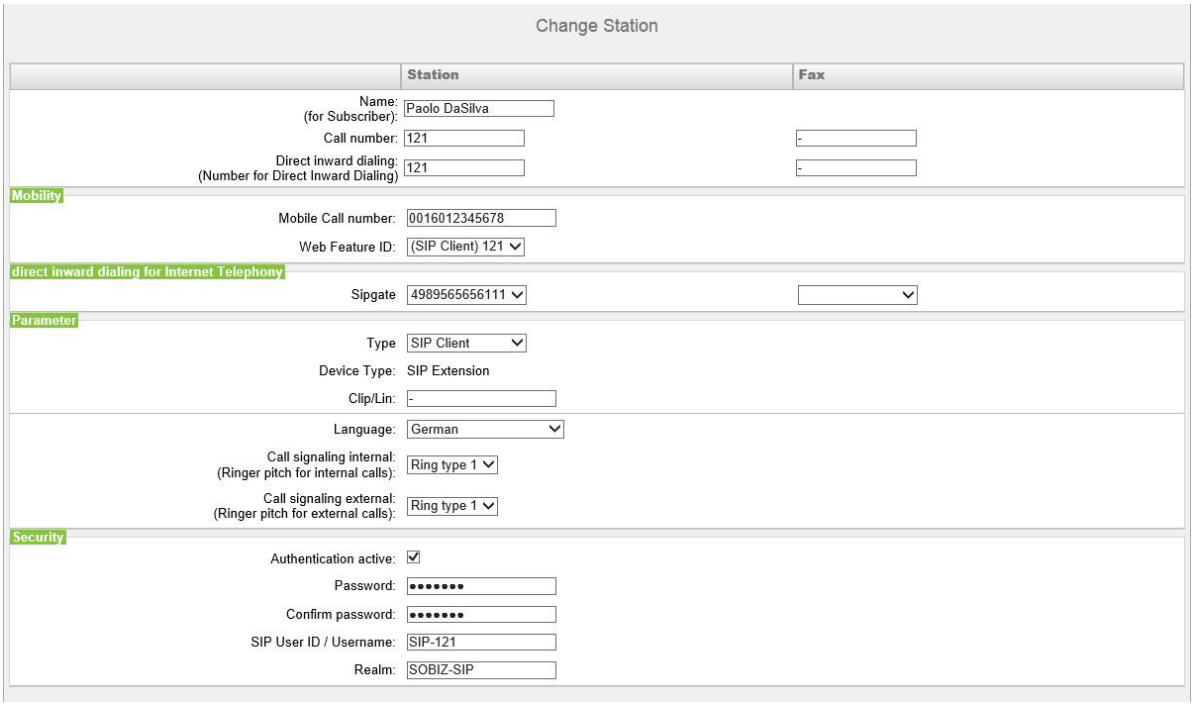
b) Wenn für die Faxbox eine Durchwahlnummer konfiguriert werden soll, geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax DuWa** die gewünschte externe Fax-Rufnummer ein, unter der der Teilnehmer von extern Faxnachrichten empfangen kann.

11) Wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Berechtigung** die gewünschte Berechtigungsklasse aus.

12) Um den Teilnehmer in eine Anrufübernahmegruppe aufzunehmen, wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Anrufübernahme** eine Anrufübernahmegruppe aus.

13) Konfigurieren Sie die Daten für die SIP-Registrierung:

a) Klicken Sie in der Zeile des gewünschten Teilnehmers auf das Stiftsymbol **Bearbeiten**.



b) Aktivieren Sie im Bereich **Sicherheit** das Kontrollkästchen **Authentifizierung aktiv**.

c) Vergeben Sie in den Feldern **Kennwort** und **Kennwort bestätigen** ein Kennwort für die Authentifizierung des SIP-Teilnehmers.

d) Vergeben Sie im Feld **SIP User ID / Benutzername** einen Benutzernamen Ihrer Wahl für die Authentifizierung des SIP-Teilnehmers, z. B. SIP-120.

e) Vergeben Sie unter **Realm** einen Namen Ihrer Wahl für die zugehörige Zone, z. B. OSBIZ-SIP. Dieser Wert sollte für alle SIP-Teilnehmer gleich sein.

INFO: Die hier definierten Werte für Kennwort, SIP User ID und Realm müssen auch am SIP-Telefon eingegeben werden.

---

14) Führen Sie bei Bedarf weitere Einstellungen durch:

a) Wenn dieses SIP-Telefon zusammen mit einem Dual-Mode-Mobiltelefon betrieben werden soll, geben Sie im Bereich Mobility unter mobile Rufnummer die Amtskennziffer und gefolgt von der Rufnummer des Mobiltelefons ein (z. B. 0016012345678). Wählen Sie zusätzlich aus der Aufklappliste Web Feature ID diesen SIP Client aus. (siehe *Dual-Mode-Telefonie*).

b) Ordnen Sie im Bereich **Durchwahl für Internet-Telefonie** dem Teilnehmer und falls gewünscht seiner Faxbox jeweils eine Durchwahlnummer für die Internet-Telefonie zu. Wählen Sie dazu aus den Aufklapplisten des gewünschten ITSP die Durchwahlnummern aus. Für jeden

aktiven ITSP wird Ihnen eine Aufklappliste für den Teilnehmer und eine Aufklappliste für seine Faxbox angezeigt.

INFO: Das Feld **Durchwahl für Internet-Telefonie** ist nicht sichtbar, wenn die Internet-Telefonie nicht eingerichtet oder kein Internet-Telefonie-Service-Provider aktiviert ist.

---

c) Geben Sie im Feld **Clip/Lin** eine Rufnummer ein (Durchwahlnummer oder MSN), die beim einem externen Anruf im Display des Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird.

INFO: Dieses Leistungsmerkmal muss vom Netzanbieter freigegeben sein.

---

d) Wählen Sie aus der Aufklappliste **Sprache** die Sprache für die Menüsteuerung des Telefons aus.

e) Weisen Sie aus der Aufklappliste **Rufsignalisierung intern** dem Teilnehmer eine von insgesamt acht möglichen akustischen Rufsignalisierungen für interne Anrufe zu. Dadurch sendet der Teilnehmer anderen internen Teilnehmern einen veränderten Rufton, durch den er von anderen Teilnehmern unterschieden werden kann (Standard: Rufart 1).

f) Weisen Sie aus der Aufklappliste **Rufsignalisierung extern** dem Teilnehmer eine von insgesamt drei möglichen akustischen Rufsignalisierungen für externe Anrufe zu (Standard: Rufart 1).

g) Nur bei UC Smart: Wählen Sie in der Aufklappliste **Mailboxtyp UC Smart** aus, ob der Teilnehmer eine Standardmailbox oder eine Vermittlungsmailbox (AutoAttendant) erhalten soll.

h) Nur bei UC Smart und Standardmailbox: Wenn ein Anrufer eine Nachricht auf der Sprachbox hinterlassen darf, aktivieren Sie das Kontrollkästchen **Aufnahme**.

i) Nur bei UC Smart: Wählen Sie aus der Aufklappliste **Begrüßung** eine Begrüßung aus.

j) Nur bei UC Smart: Wenn das Kennwort der Sprachbox zurückgesetzt werden soll, aktivieren Sie das Kontrollkästchen **Passwort Reset**.

INFO: Das Kontrollkästchen **Passwort Reset** muss bei einer Neueinrichtung einer Sprachbox nicht gesetzt sein. Es bewirkt das Rücksetzen des Kennworts der Sprachbox. Bei einer Neueinrichtung muss der Teilnehmer sowieso beim ersten Zugriff auf seine Sprachbox das Initial-Kennwort ändern.

---

k) Klicken Sie auf **OK & Weiter**.

15) Wenn Sie einen weiteren Teilnehmer einrichten möchten, wiederholen Sie die Schritte 5 bis 14.

16) Klicken Sie auf **OK & Weiter**. Sie sehen eine Liste aller eingerichteten IP-Teilnehmer. Bei Bedarf können Sie sich mit **Drucken** die Liste der IP-Teilnehmer ausdrucken.

17) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

10.12.3 Wie Sie UP0-Teilnehmer konfigurieren

Mit dem Wizard **UP0-Endgeräte** können Sie die UP0-Teilnehmer konfigurieren.

Voraussetzungen

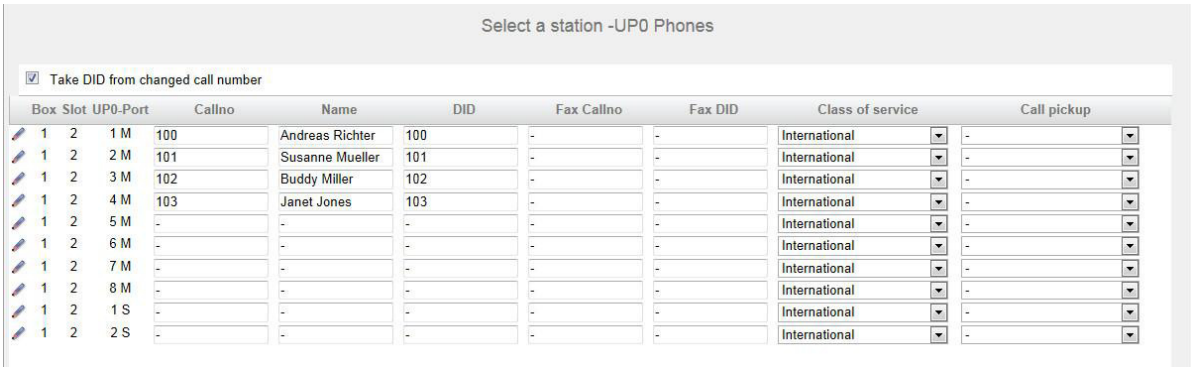
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Endgeräte/Teilnehmer**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **UP0-Endgeräte** zu starten. Es wird Ihnen eine Liste aller UP0-Teilnehmer angezeigt.



4) Wenn der Teilnehmer automatisch als Durchwahlnummer die interne Rufnummer bekommen soll, aktivieren Sie das Optionsfeld **Durchwahl bei Eingabe der Rufnummer übernehmen**.

5) Wenn sich die Durchwahlnummer des Teilnehmers von seiner Rufnummer unterscheiden soll, geben Sie in der Zeile des gewünschten Teilnehmers unter **DuWa** eine Durchwahl-Nummer für den Teilnehmer ein:

- nur bei Anlagenanschluss:

  Klicken Sie in das gewünschte Feld und geben Sie über die Tastatur die Durchwahlnummer ein. Die Durchwahlnummer kann auch mit der internen Rufnummer identisch sein.

- nur bei Mehrgeräteanschluss:

  Wählen Sie in dem gewünschten Feld über die Aufklappliste eine MSN aus. Der Teilnehmer kann z. B. von intern über die interne Rufnummer 101 und von extern über die MSN 654321 erreicht werden.

- bei Anlagenanschluss und Mehrgeräteanschluss:

  Wählen Sie in dem gewünschten Feld über die Aufklappliste den Eintrag **xxx - änderbar** aus (xxx steht für die interne Rufnummer) und geben Sie über die Tastatur die Durchwahlnummer ein oder wählen Sie über die Aufklappliste eine MSN aus.

6) Wenn der Teilnehmer eine Internet-Telefonie-Teilnehmerrufnummer als Durchwahlnummer erhalten soll, lassen Sie das Optionsfeld **Durchwahl bei Eingabe der Rufnummer übernehmen** deaktiviert, wählen Sie aus der Liste neben diesem Optionsfeld den Internet-Telefonie-Service-Provider aus und wählen in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **DuWa** die Internet-Telefonie-Teilnehmerrufnummer aus.

7) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Rufnr** eine interne Rufnummer für den Teilnehmer ein. Sie können die vorbelegte Rufnummer verwenden oder eine andere, noch nicht belegte Rufnummer vergeben.

8) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Name** einen Namen in der Form `Nachname,Vorname` oder `Vorname Nachname` ein.

9) Wenn für den Teilnehmer eine Faxbox eingerichtet werden soll (nutzbar z. B. mit den UC Clients **myPortal for Desktop** oder **myPortal for Outlook**), gehen Sie folgendermaßen vor:

a) Geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax Rufnr** die gewünschte interne Fax-Rufnummer ein, unter der der Teilnehmer von intern Faxnachrichten empfangen kann.

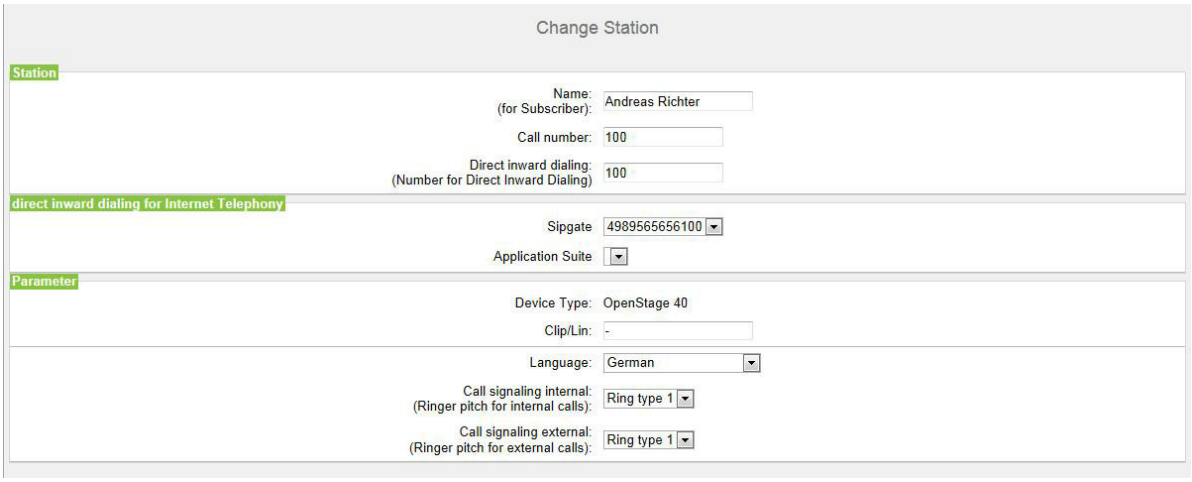
b) Wenn für die Faxbox eine Durchwahlnummer konfiguriert werden soll, geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax DuWa** die gewünschte externe Fax-Rufnummer ein, unter der der Teilnehmer von extern Faxnachrichten empfangen kann.

10) Wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Berechtigung** die gewünschte Berechtigungsklasse aus.

11) Um den Teilnehmer in eine Anrufübernahmegruppe aufzunehmen, wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Anrufübernahme** eine Anrufübernahmegruppe aus.

12) Führen Sie bei Bedarf weitere Einstellungen durch:

a) Klicken Sie in der Zeile des gewünschten Teilnehmers auf das Stiftsymbol **Bearbeiten**.



b) Wählen Sie im Bereich **Durchwahl für Internet-Telefonie** aus einer Aufklappliste eine Durchwahlnummer aus. Für jeden aktiven ITSP wird Ihnen eine Aufklappliste angezeigt.

INFO: Das Feld **Durchwahl für Internet-Telefonie** ist nicht sichtbar, wenn die Internet-Telefonie nicht eingerichtet oder kein Internet-Telefonie-Service-Provider aktiviert ist.

---

c) Geben Sie im Feld **Clip/Lin** eine Rufnummer ein (Durchwahlnummer oder MSN), die beim einem externen Anruf im Display des Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird.

INFO: Dieses Leistungsmerkmal muss vom Netzanbieter freigegeben sein.

---

d) Wählen Sie aus der Aufklappliste **Sprache** die Sprache für die Menüsteuerung des Telefons aus.

e) Weisen Sie aus der Aufklappliste **Rufsignalisierung intern** dem Teilnehmer eine von insgesamt acht möglichen akustischen Rufsignalisierungen für interne Anrufe zu. Dadurch sendet der Teilnehmer anderen internen Teilnehmern einen veränderten Rufton, durch den er von anderen Teilnehmern unterschieden werden kann (Standard: Rufart 1).

f) Weisen Sie aus der Aufklappliste **Rufsignalisierung extern** dem Teilnehmer eine von insgesamt drei möglichen akustischen Rufsignalisierungen für externe Anrufe zu (Standard: Rufart 1).

g) Nur bei UC Smart: Wählen Sie in der Aufklappliste **Mailboxtyp UC Smart** aus, ob der Teilnehmer eine Standardmailbox oder eine Vermittlungsmailbox (AutoAttendant) erhalten soll.

h) Nur bei UC Smart und Standardmailbox: Wenn ein Anrufer eine Nachricht auf der Sprachbox hinterlassen darf, aktivieren Sie das Kontrollkästchen **Aufnahme**.

i) Nur bei UC Smart: Wählen Sie aus der Aufklappliste **Begrüßung** eine Begrüßung aus.

j) Nur bei UC Smart: Wenn das Kennwort der Sprachbox zurückgesetzt werden soll, aktivieren Sie das Kontrollkästchen **Passwort Reset**.

INFO: Das Kontrollkästchen **Passwort Reset** muss bei einer Neueinrichtung einer Sprachbox nicht gesetzt sein. Es bewirkt das Rücksetzen des Kennworts der Sprachbox. Bei einer Neueinrichtung muss der Teilnehmer sowieso beim ersten Zugriff auf seine Sprachbox das Initial-Kennwort ändern.

---

k) Klicken Sie auf **OK & Weiter**.

13) Wenn Sie einen weiteren Teilnehmer einrichten möchten, wiederholen Sie die Schritte 5 bis 12.

14) Klicken Sie auf **OK & Weiter**. Sie sehen eine Liste aller eingerichteten UP0-Teilnehmer. Bei Bedarf können Sie sich mit **Drucken** die Liste der UP0-Teilnehmer ausdrucken.

15) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

10.12.4 Wie Sie DECT-Teilnehmer konfigurieren

Mit dem Wizard **DECT-Endgeräte** können Sie die DECT-Teilnehmer (DECT-Telefone) konfigurieren.

Voraussetzungen

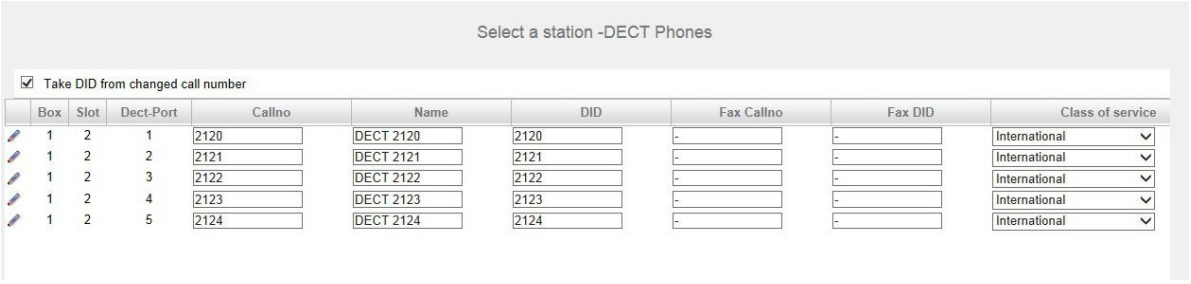
- Eine Basisstation ist an einer UP0-Schnittstelle oder an einer gesteckten SLC-Baugruppe angeschlossen.
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Endgeräte/Teilnehmer**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **DECT-Endgeräte** zu starten. Es wird Ihnen eine Liste aller DECT-Teilnehmer angezeigt.



4) Wenn der Teilnehmer automatisch als Durchwahlnummer die interne Rufnummer bekommen soll, aktivieren Sie das Optionsfeld **Durchwahl bei Eingabe der Rufnummer übernehmen**.

5) Wenn sich die Durchwahlnummer des Teilnehmers von seiner Rufnummer unterscheiden soll, geben Sie in der Zeile des gewünschten Teilnehmers unter **DuWa** eine Durchwahl-Nummer für den Teilnehmer ein:

- nur bei Anlagenanschluss:

  Klicken Sie in das gewünschte Feld und geben Sie über die Tastatur die Durchwahlnummer ein. Die Durchwahlnummer kann auch mit der internen Rufnummer identisch sein.

- nur bei Mehrgeräteanschluss:

  Wählen Sie in dem gewünschten Feld über die Aufklappliste eine MSN aus. Der Teilnehmer kann z. B. von intern über die interne Rufnummer 101 und von extern über die MSN 654321 erreicht werden.

- bei Anlagenanschluss und Mehrgeräteanschluss:

  Wählen Sie in dem gewünschten Feld über die Aufklappliste den Eintrag **xxx - änderbar** aus (xxx steht für die interne Rufnummer) und geben Sie über die Tastatur die Durchwahlnummer ein oder wählen Sie über die Aufklappliste eine MSN aus.

6) Wenn der Teilnehmer eine Internet-Telefonie-Teilnehmerrufnummer als Durchwahlnummer erhalten soll, lassen Sie das Optionsfeld **Durchwahl bei Eingabe der Rufnummer übernehmen** deaktiviert, wählen Sie aus der Liste neben diesem Optionsfeld den Internet-Telefonie-Service-Provider aus und wählen in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **DuWa** die Internet-Telefonie-Teilnehmerrufnummer aus.

7) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Rufnr** eine interne Rufnummer für den Teilnehmer ein. Sie können die vorbelegte Rufnummer verwenden oder eine andere, noch nicht belegte Rufnummer vergeben.

8) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Name** einen Namen in der Form `Nachname,Vorname` oder `Vorname Nachname` ein.

9) Wenn für den Teilnehmer eine Faxbox eingerichtet werden soll (nutzbar z. B. mit den UC Clients **myPortal for Desktop** oder **myPortal for Outlook**), gehen Sie folgendermaßen vor:

a) Geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax Rufnr** die gewünschte interne Fax-Rufnummer ein, unter der der Teilnehmer von intern Faxnachrichten empfangen kann.

b) Wenn für die Faxbox eine Durchwahlnummer konfiguriert werden soll, geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax DuWa** die gewünschte externe Fax-Rufnummer ein, unter der der Teilnehmer von extern Faxnachrichten empfangen kann.

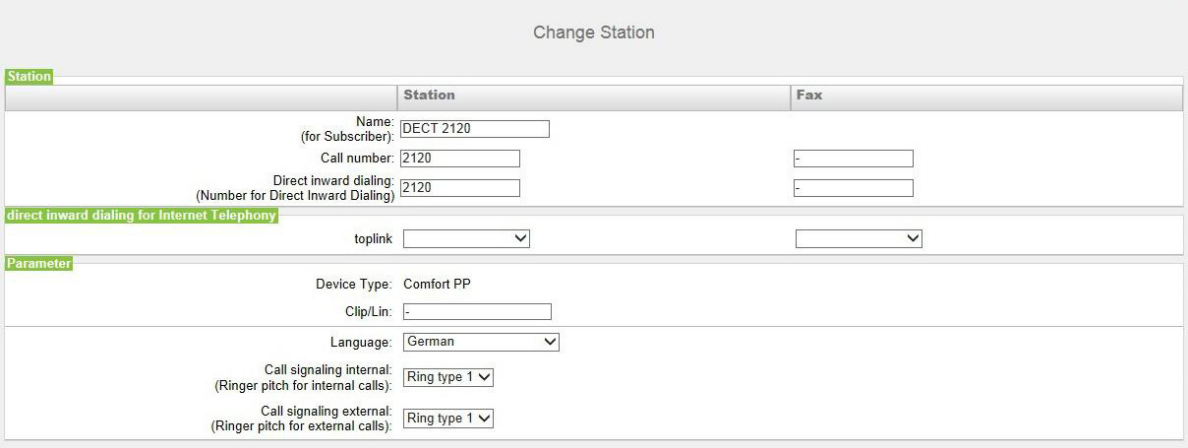
10) Wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Berechtigung** die gewünschte Berechtigungsklasse aus.

11) Um den Teilnehmer in eine Anrufübernahmegruppe aufzunehmen, wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Anrufübernahme** eine Anrufübernahmegruppe aus.

12) Falls Sie den DECT-Telefoncode (PIN) ändern wollen, geben Sie in der Zeile des gewünschten Teilnehmers unter **Mobilcode** den neuen Code ein. Der DECT-Teilnehmer muss sich mit diesem Code neu an der Basisstation anmelden.

13) Führen Sie bei Bedarf weitere Einstellungen durch:

a) Klicken Sie in der Zeile des gewünschten Teilnehmers auf das Stiftsymbol **Bearbeiten**.



b) Wählen Sie im Bereich **Durchwahl für Internet-Telefonie** aus einer Aufklappliste eine Durchwahlnummer aus. Für jeden aktiven ITSP wird Ihnen eine Aufklappliste angezeigt.

INFO: Das Feld **Durchwahl für Internet-Telefonie** ist nicht sichtbar, wenn die Internet-Telefonie nicht eingerichtet oder kein Internet-Telefonie-Service-Provider aktiviert ist.

---

c) Geben Sie im Feld **Clip/Lin** eine Rufnummer ein (Durchwahlnummer oder MSN), die beim einem externen Anruf im Display des Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird.

INFO: Dieses Leistungsmerkmal muss vom Netzanbieter freigegeben sein.

---

d) Wählen Sie aus der Aufklappliste **Sprache** die Sprache für die Menüsteuerung des Telefons aus.

e) Weisen Sie aus der Aufklappliste **Rufsignalisierung intern** dem Teilnehmer eine von insgesamt acht möglichen akustischen Rufsignalisierungen für interne Anrufe zu. Dadurch sendet der Teilnehmer anderen internen Teilnehmern einen veränderten Rufton, durch den er von anderen Teilnehmern unterschieden werden kann (Standard: Rufart 1).

f) Weisen Sie aus der Aufklappliste **Rufsignalisierung extern** dem Teilnehmer eine von insgesamt drei möglichen akustischen Rufsignalisierungen für externe Anrufe zu (Standard: Rufart 1).

g) Nur bei UC Smart: Wählen Sie in der Aufklappliste **Mailboxtyp UC Smart** aus, ob der Teilnehmer eine Standardmailbox oder eine Vermittlungsmailbox (AutoAttendant) erhalten soll.

h) Nur bei UC Smart und Standardmailbox: Wenn ein Anrufer eine Nachricht auf der Sprachbox hinterlassen darf, aktivieren Sie das Kontrollkästchen **Aufnahme**.

i) Nur bei UC Smart: Wählen Sie aus der Aufklappliste **Begrüßung** eine Begrüßung aus.

j) Nur bei UC Smart: Wenn das Kennwort der Sprachbox zurückgesetzt werden soll, aktivieren Sie das Kontrollkästchen **Passwort Reset**.

INFO: Das Kontrollkästchen **Passwort Reset** muss bei einer Neueinrichtung einer Sprachbox nicht gesetzt sein. Es bewirkt das Rücksetzen des Kennworts der Sprachbox. Bei einer Neueinrichtung muss der Teilnehmer sowieso beim ersten Zugriff auf seine Sprachbox das Initial-Kennwort ändern.

---

k) Klicken Sie auf **OK & Weiter**.

14) Wenn Sie einen weiteren Teilnehmer einrichten möchten, wiederholen Sie die Schritte5 bis 13.

15) Klicken Sie auf **OK & Weiter**. Sie sehen eine Liste aller eingerichteten DECT-Teilnehmer. Bei Bedarf können Sie sich mit **Drucken** die Liste der DECT-Teilnehmer ausdrucken.

16) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

10.12.5 Wie Sie ISDN-Teilnehmer konfigurieren

Mit dem Wizard **ISDN-Endgeräte** können Sie die ISDN-Teilnehmer (z. B. ISDN-Telefon oder ISDN-Fax) konfigurieren.

Voraussetzungen

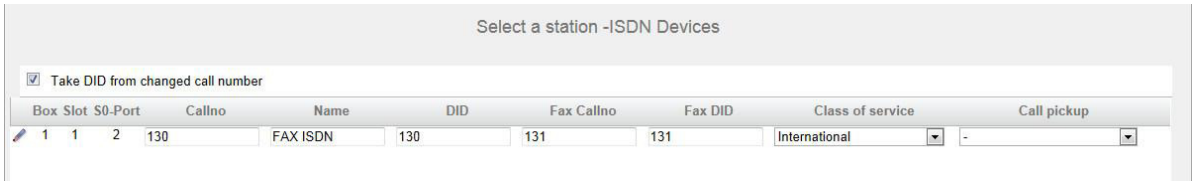
- Es ist mindestens eine freie S_0-Schnittstelle vorhanden. Wird einer der S_0-Ports einer Hardware-Plattform genutzt, muss dieser als interner S_0-Anschluss eingerichtet sein.
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Endgeräte / Teilnehmer**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **ISDN-Endgeräte** zu starten. Es wird Ihnen eine Liste aller ISDN-Teilnehmer angezeigt.



4) Wenn die Durchwahlnummer des Teilnehmers automatisch seiner Rufnummer angepasst werden soll, aktivieren Sie das Optionsfeld **Durchwahl bei Eingabe der Rufnummer übernehmen**.

5) Wenn sich die Durchwahlnummer des Teilnehmers von seiner Rufnummer unterscheiden soll, geben Sie in der Zeile des gewünschten Teilnehmers unter **DuWa** eine Durchwahl-Nummer für den Teilnehmer ein:

- nur bei Anlagenanschluss:

  Klicken Sie in das gewünschte Feld und geben Sie über die Tastatur die Durchwahlnummer ein. Die Durchwahlnummer kann auch mit der internen Rufnummer identisch sein.

- nur bei Mehrgeräteanschluss:

  Wählen Sie in dem gewünschten Feld über die Aufklappliste eine MSN aus. Der Teilnehmer kann z. B. von intern über die interne Rufnummer 101 und von extern über die MSN 654321 erreicht werden.

- bei Anlagenanschluss und Mehrgeräteanschluss:

  Wählen Sie in dem gewünschten Feld über die Aufklappliste den Eintrag **xxx - änderbar** aus (xxx steht für die interne Rufnummer) und geben Sie über die Tastatur die Durchwahlnummer ein oder wählen Sie über die Aufklappliste eine MSN aus.

6) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Rufnr** eine interne Rufnummer für den Teilnehmer ein. Sie können die vorbelegte Rufnummer verwenden oder eine andere, noch nicht belegte Rufnummer vergeben.

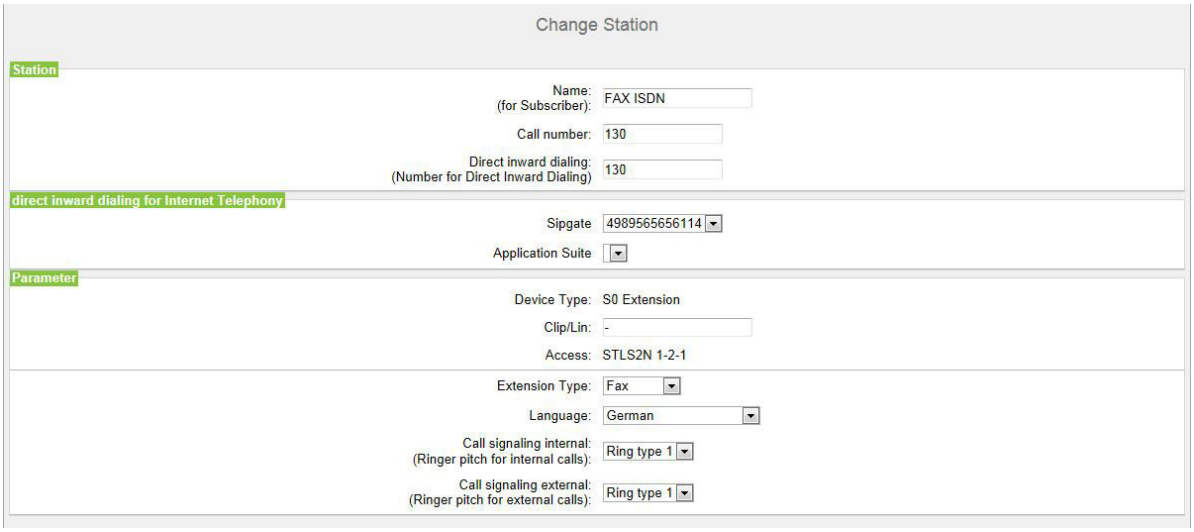
7) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Name** einen Namen in der Form `Nachname,Vorname` oder `Vorname Nachname` ein.

8) Wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Berechtigung** eine der gewünschten Berechtigungsgruppen aus.

9) Um den Teilnehmer in eine Anrufübernahmegruppe aufzunehmen, wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Anrufübernahme** eine Anrufübernahmegruppe aus.

10) Führen Sie bei Bedarf weitere Einstellungen durch:

a) Klicken Sie in der Zeile des gewünschten Teilnehmers auf das Stiftsymbol **Bearbeiten**.



b) Wählen Sie im Bereich **Durchwahl für Internet-Telefonie** aus einer Aufklappliste eine Durchwahlnummer aus. Für jeden aktiven ITSP wird Ihnen eine Aufklappliste angezeigt.

INFO: Das Feld **Durchwahl für Internet-Telefonie** ist nicht sichtbar, wenn die Internet-Telefonie nicht eingerichtet oder kein Internet-Telefonie-Service-Provider aktiviert ist.

---

c) Geben Sie im Feld **Clip/Lin** eine Rufnummer ein (Durchwahlnummer oder MSN), die beim einem externen Anruf im Display des Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird.

INFO: Dieses Leistungsmerkmal muss vom Netzanbieter freigegeben sein.

---

d) Wählen Sie aus der Aufklappliste **Stationstyp** den Typ des ISDN-Endgeräts aus (`Standard` oder `Fax`).

e) Belassen Sie die Standard-Auswahl in der Aufklappliste **Sprache**. Für ISDN-Endgeräte ist diese Einstellung ohne Bedeutung.

f) Weisen Sie aus der Aufklappliste **Rufsignalisierung intern** dem Teilnehmer eine von insgesamt acht möglichen akustischen Rufsignalisierungen für interne Anrufe zu. Dadurch sendet der Teilnehmer anderen internen Teilnehmern einen veränderten Rufton, durch den er von anderen Teilnehmern unterschieden werden kann (Standard: Rufart 1).

g) Weisen Sie aus der Aufklappliste **Rufsignalisierung extern** dem Teilnehmer eine von insgesamt drei möglichen akustischen Rufsignalisierungen für externe Anrufe zu (Standard: Rufart 1).

h) Nur bei UC Smart: Wählen Sie in der Aufklappliste **Mailboxtyp UC Smart** aus, ob der Teilnehmer eine Standardmailbox oder eine Vermittlungsmailbox (AutoAttendant) erhalten soll.

i) Nur bei UC Smart und Standardmailbox: Wenn ein Anrufer eine Nachricht auf der Sprachbox hinterlassen darf, aktivieren Sie das Kontrollkästchen **Aufnahme**.

j) Nur bei UC Smart: Wählen Sie aus der Aufklappliste **Begrüßung** eine Begrüßung aus.

k) Nur bei UC Smart: Wenn das Kennwort der Sprachbox zurückgesetzt werden soll, aktivieren Sie das Kontrollkästchen **Passwort Reset**.

INFO: Das Kontrollkästchen **Passwort Reset** muss bei einer Neueinrichtung einer Sprachbox nicht gesetzt sein. Es bewirkt das Rücksetzen des Kennworts der Sprachbox. Bei einer Neueinrichtung muss der Teilnehmer sowieso beim ersten Zugriff auf seine Sprachbox das Initial-Kennwort ändern.

---

l) Klicken Sie auf **OK & Weiter**.

11) Wenn Sie einen weiteren Teilnehmer einrichten möchten, wiederholen Sie die Schritte 5 bis 10.

12) Klicken Sie auf **OK & Weiter**. Sie sehen eine Liste aller eingerichteten ISDN-Teilnehmer. Bei Bedarf können Sie sich mit **Drucken** die Liste der ISDN-Teilnehmer ausdrucken.

13) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

10.12.6 Wie Sie analoge Teilnehmer konfigurieren

Mit dem Wizard **Analog-Endgeräte** können Sie analoge Teilnehmer (z. B. analoges Telefon oder analoges Fax) einrichten.

Voraussetzungen

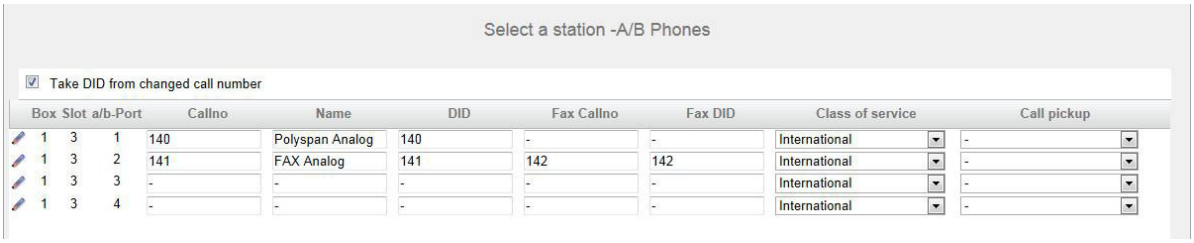
- Es ist mindestens eine freie analoge Schnittstelle vorhanden.
- An den analogen Geräten ist MFV aktiviert.
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Endgeräte / Teilnehmer**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Analog-Endgeräte** zu starten. Es wird Ihnen eine Liste aller analogen Teilnehmer angezeigt.



4) Wenn die Durchwahlnummer des Teilnehmers automatisch seiner Rufnummer angepasst werden soll, aktivieren Sie das Optionsfeld **Durchwahl bei Eingabe der Rufnummer übernehmen**.

5) Wenn sich die Durchwahlnummer des Teilnehmers von seiner Rufnummer unterscheiden soll, geben Sie in der Zeile des gewünschten Teilnehmers unter **DuWa** eine Durchwahl-Nummer für den Teilnehmer ein:

- nur bei Anlagenanschluss:

  Klicken Sie in das gewünschte Feld und geben Sie über die Tastatur die Durchwahlnummer ein. Die Durchwahlnummer kann auch mit der internen Rufnummer identisch sein.

- nur bei Mehrgeräteanschluss:

  Wählen Sie in dem gewünschten Feld über die Aufklappliste eine MSN aus. Der Teilnehmer kann z. B. von intern über die interne Rufnummer 101 und von extern über die MSN 654321 erreicht werden.

- bei Anlagenanschluss und Mehrgeräteanschluss:

  Wählen Sie in dem gewünschten Feld über die Aufklappliste den Eintrag **xxx - änderbar** aus (xxx steht für die interne Rufnummer) und geben Sie über die Tastatur die Durchwahlnummer ein oder wählen Sie über die Aufklappliste eine MSN aus.

6) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Rufnr** eine interne Rufnummer für den Teilnehmer ein. Sie können die vorbelegte Rufnummer verwenden oder eine andere, noch nicht belegte Rufnummer vergeben.

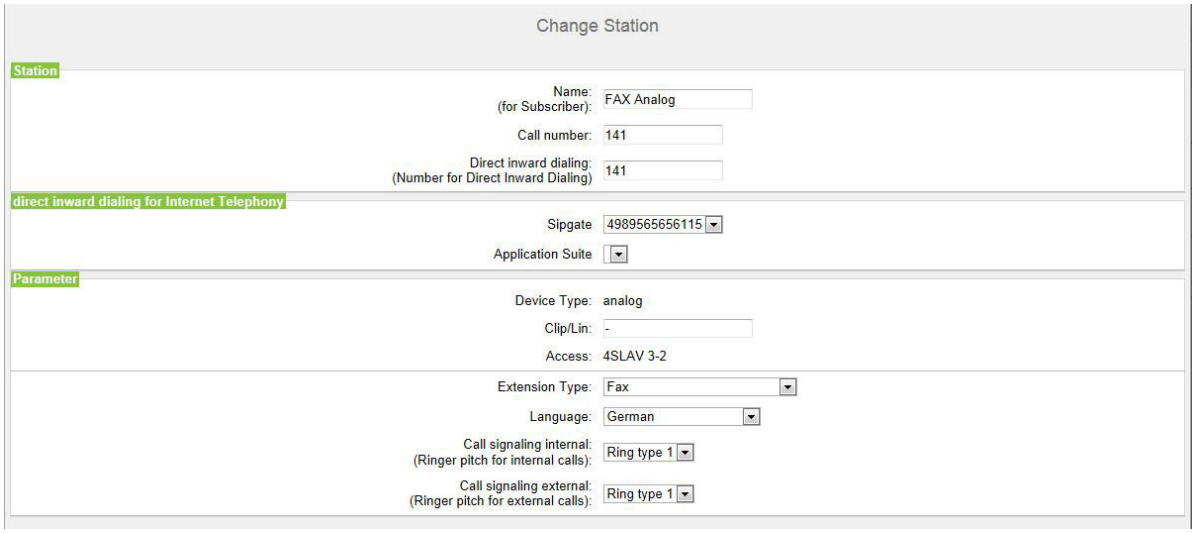
7) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Name** einen Namen in der Form `Nachname,Vorname` oder `Vorname Nachname` ein.

8) Wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Berechtigung** eine der gewünschten Berechtigungsgruppen aus.

9) Um den Teilnehmer in eine Anrufübernahmegruppe aufzunehmen, wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Anrufübernahme** eine Anrufübernahmegruppe aus.

10) Führen Sie bei Bedarf weitere Einstellungen durch - für ein analoges Modem muss hier der Stationstyp **Modem** ausgewählt werden:

a) Klicken Sie in der Zeile des gewünschten Teilnehmers auf das Stiftsymbol **Bearbeiten**.



b) Wählen Sie im Bereich **Durchwahl für Internet-Telefonie** aus einer Aufklappliste eine Durchwahlnummer aus. Für jeden aktiven ITSP wird Ihnen eine Aufklappliste angezeigt.

INFO: Das Feld **Durchwahl für Internet-Telefonie** ist nicht sichtbar, wenn die Internet-Telefonie nicht eingerichtet oder kein Internet-Telefonie-Service-Provider aktiviert ist.

---

c) Geben Sie im Feld **Clip/Lin** eine Rufnummer ein (Durchwahlnummer oder MSN), die beim einem externen Anruf im Display des Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird.

INFO: Dieses Leistungsmerkmal muss vom Netzanbieter freigegeben sein.

---

d) Wählen Sie aus der Aufklappliste **Stationstyp** den Typ des analogen Endgeräts (z. B. **Fax**) aus.

Soll ein analoges Modem eingerichtet werden, ist hier der Stationstyp **Modem** auszuwählen.

e) Belassen Sie die Standard-Auswahl in der Aufklappliste **Sprache**. Für analoge Endgeräte ist diese Einstellung ohne Bedeutung.

f) Weisen Sie aus der Aufklappliste **Rufsignalisierung intern** dem Teilnehmer eine von insgesamt acht möglichen akustischen Rufsignalisierungen für interne Anrufe zu. Dadurch sendet der Teilnehmer anderen internen Teilnehmern einen veränderten Rufton, durch den er von anderen Teilnehmern unterschieden werden kann (Standard: Rufart 1).

g) Weisen Sie aus der Aufklappliste **Rufsignalisierung extern** dem Teilnehmer eine von insgesamt drei möglichen akustischen Rufsignalisierungen für externe Anrufe zu (Standard: Rufart 1).

h) Nur bei UC Smart: Wählen Sie in der Aufklappliste **Mailboxtyp UC Smart** aus, ob der Teilnehmer eine Standardmailbox oder eine Vermittlungsmailbox (AutoAttendant) erhalten soll.

i) Nur bei UC Smart und Standardmailbox: Wenn ein Anrufer eine Nachricht auf der Sprachbox hinterlassen darf, aktivieren Sie das Kontrollkästchen **Aufnahme**.

j) Nur bei UC Smart: Wählen Sie aus der Aufklappliste **Begrüßung** eine Begrüßung aus.

k) Nur bei UC Smart: Wenn das Kennwort der Sprachbox zurückgesetzt werden soll, aktivieren Sie das Kontrollkästchen **Passwort Reset**.

INFO: Das Kontrollkästchen **Passwort Reset** muss bei einer Neueinrichtung einer Sprachbox nicht gesetzt sein. Es bewirkt das Rücksetzen des Kennworts der Sprachbox. Bei einer Neueinrichtung muss der Teilnehmer sowieso beim ersten Zugriff auf seine Sprachbox das Initial-Kennwort ändern.

---

l) Klicken Sie auf **OK & Weiter**.

11) Wenn Sie einen weiteren Teilnehmer einrichten möchten, wiederholen Sie die Schritte 5 bis 10.

12) Klicken Sie auf **OK & Weiter**. Sie sehen eine Liste aller eingerichteten analogen Teilnehmer. Bei Bedarf können Sie sich mit **Drucken** die Liste der analogen Teilnehmer ausdrucken.

13) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

10.12.7 Wie Sie den Namen der Teilnehmer ändern

Mit dem Wizard **Teilnehmername und Freischaltung** können Sie die Namen der Teilnehmer ändern.

Voraussetzungen

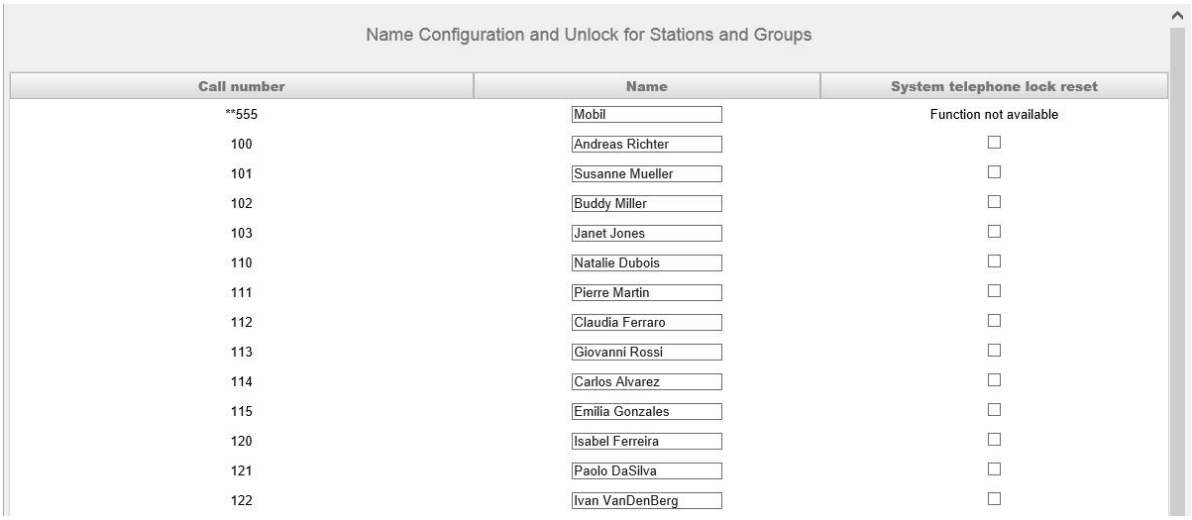
- Sie sind am WBM angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > User-Telefonie**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Teilnehmername und Freischaltung** zu starten.



4) Klicken Sie in der Spalte **Name** in das Feld des gewünschten Teilnehmers und ändern Sie den Namen des Teilnehmers in der Form `Nachname, Vorname` oder `Vorname Nachname`.

5) Wenn Sie die Namen weiterer Teilnehmer ändern wollen, wiederholen Sie den Schritt 4.

6) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

10.13 Konfiguration der Teilnehmer-Profile

In Teilnehmer-Profilen werden die Werte und Eigenschaften der IP-Teilnehmer abgespeichert.

Über den Wizard **Profile** kann ein Administrator mit dem Profil **Advanced** folgende Konfigurationen durchführen:

- Neues Profil anlegen
- Profile und deren Mitglieder anzeigen
- Mitglieder zu einem Profil hinzufügen
- Mitglieder aus einem Profil löschen
- Einzelnes Profil exportieren oder importieren

Über den Experten-Modus kann ein Administrator mit dem Profil **Expert** zusätzlich folgende Konfigurationen durchführen:

- Werte und Einstellungen eines bestehenden Profils ändern
- Alle Profile exportieren oder importieren

Bereits angelegte Teilnehmer-Profile können nicht gelöscht, aber überschrieben werden.

10.13.1 Wie Sie ein neues Teilnehmer-Profil anlegen

Voraussetzungen

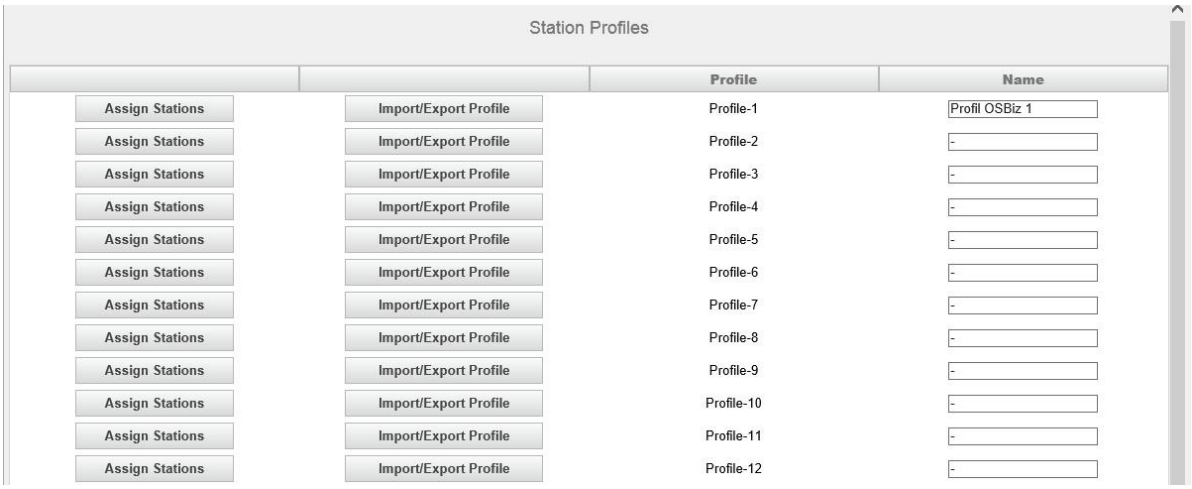
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

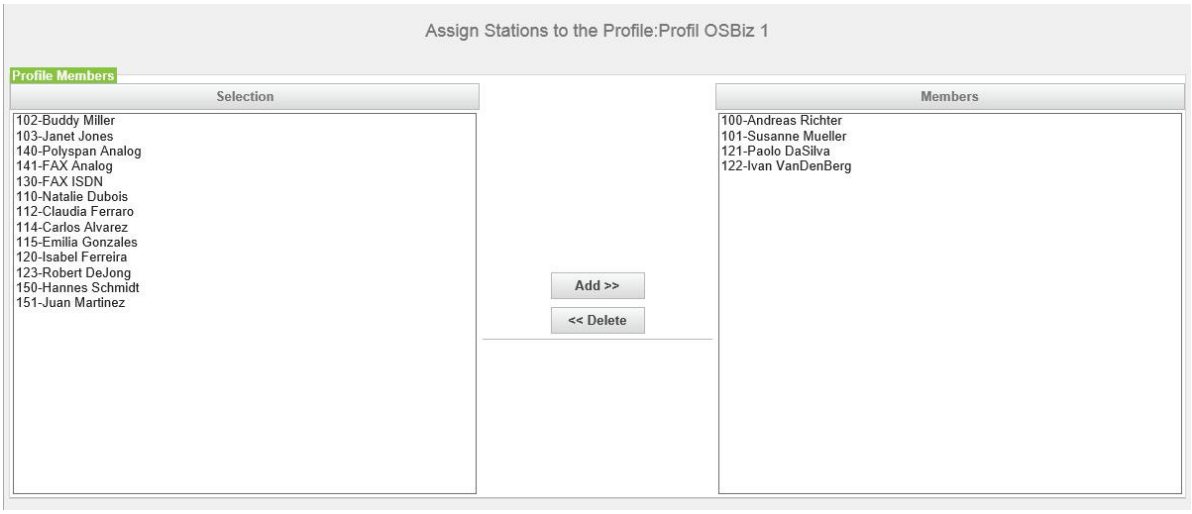
2) Klicken Sie im Navigationsbaum auf **Wizards > User-Telefonie**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Teilnehmer-Profile** zu starten. Es werden Ihnen alle vorhandenen Teilnehmer-Profile angezeigt.



4) Geben Sie in der Zeile des gewünschten Teilnehmer-Profils in der Spalte **Name** einen frei wählbaren Namen für das Profil an (max. 16 Stellen möglich).

5) Klicken Sie in der Zeile des gewünschten Teilnehmer-Profils auf **Teilnehmer zuordnen**.



6) Wählen Sie aus der Tabelle **Profile Mitglieder** die gewünschten Mitglieder aus (Mehrfachauswahl ist möglich) und klicken Sie auf **Hinzufügen**. Diese

Teilnehmer sind dem Teilnehmer-Profil zugeordnet und können keinem weiteren Teilnehmer-Profil zugewiesen werden.

7) Klicken Sie auf **OK**.

8) Klicken Sie auf **OK & Weiter**. Es werden Ihnen alle vorhandenen Teilnehmer-Profile und deren Mitglieder angezeigt.

9) Klicken Sie auf **OK & Weiter** und abschließend auf **Beenden**.

10.13.2 Wie Sie Teilnehmer-Profile und deren Mitglieder anzeigen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > User-Telefonie**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Teilnehmer-Profile** zu starten. Es werden Ihnen alle vorhandenen Teilnehmer-Profile angezeigt.

4) Klicken Sie auf **OK & Weiter**. Es werden Ihnen alle vorhandenen Teilnehmer-Profile und deren Mitglieder angezeigt.

10.13.3 Wie Sie Mitglieder zu einem Teilnehmer-Profil hinzufügen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > User-Telefonie**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Teilnehmer-Profile** zu starten. Es werden Ihnen alle vorhandenen Teilnehmer-Profile und deren Mitglieder angezeigt.

4) Klicken Sie in der Zeile des gewünschten Teilnehmer-Profils auf **Teilnehmer zuordnen**.



5) Wählen Sie aus der Liste **Profile Mitglieder** die gewünschten Mitglieder aus (Mehrfachauswahl ist möglich) und klicken Sie auf **Hinzufügen**. Diese Teilnehmer sind dem Teilnehmer-Profil zugeordnet und können keinem weiteren Teilnehmer-Profil zugewiesen werden.

6) Klicken Sie auf **OK**.

7) Klicken Sie auf **OK & Weiter**. Es werden Ihnen alle vorhandenen Teilnehmer-Profile und deren Mitglieder angezeigt.

8) Klicken Sie auf **OK & Weiter** und abschließend auf **Beenden**.

10.13.4 Wie Sie Mitglieder aus einem Teilnehmer-Profil löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

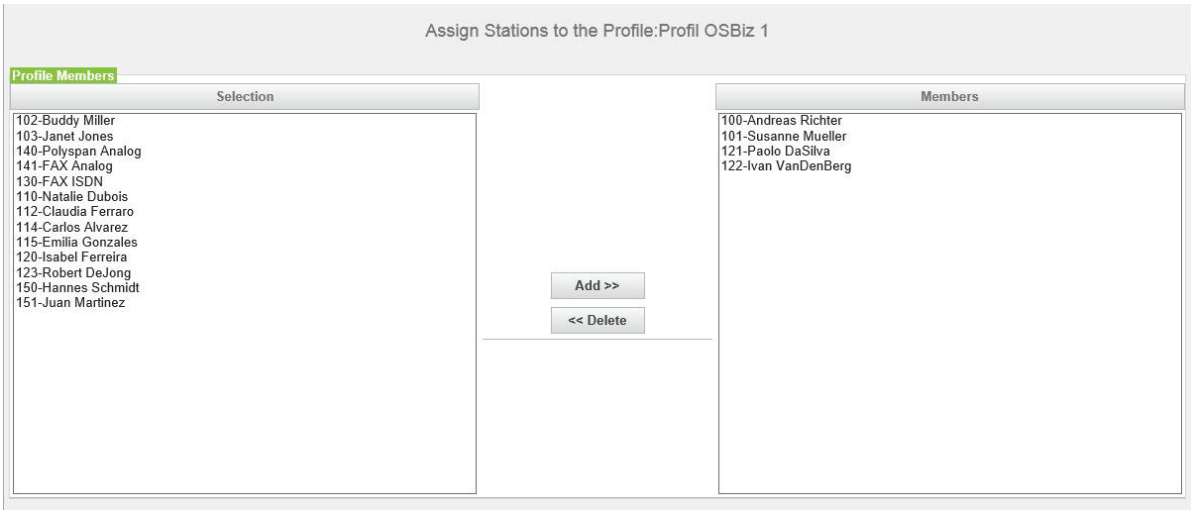
Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > User-Telefonie**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Teilnehmer-Profile** zu starten. Es werden Ihnen alle vorhandenen Teilnehmer-Profile und deren Mitglieder angezeigt.

4) Klicken Sie in der Zeile des gewünschten Teilnehmer-Profils auf **Teilnehmer zuordnen**.



5) Wählen Sie aus der Liste **Mitglieder** die gewünschten Mitglieder aus (Mehrfachauswahl ist möglich) und klicken Sie auf **Löschen**. Diese Teilnehmer können wieder einem anderen Teilnehmer-Profil zugewiesen werden.

6) Klicken Sie auf **OK**.

7) Klicken Sie auf **OK & Weiter**. Es werden Ihnen alle vorhandenen Teilnehmer-Profile und deren Mitglieder angezeigt.

8) Klicken Sie auf **OK & Weiter** und abschließend auf **Beenden**.

10.13.5 Wie Sie ein einzelnes Teilnehmer-Profil exportieren oder importieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > User-Telefonie**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Teilnehmer-Profile** zu starten. Es werden Ihnen alle vorhandenen Teilnehmer-Profile und deren Mitglieder angezeigt.

4) Klicken Sie in der Zeile des gewünschten Teilnehmer-Profils auf **Profil importieren/exportieren**.

5) Wenn Sie das Teilnehmer-Profil in eine Datei exportieren wollen, klicken Sie auf **Download** und speichern die Datei in einem Verzeichnis Ihrer Wahl.

6) Wenn Sie ein Teilnehmer-Profil aus einer Datei importieren wollen, klicken Sie auf **Durchsuchen**, navigieren Sie zum Ablageort der Datei und laden Sie die Datei in das Kommunikationssystem.

7) Klicken Sie auf **OK**.

8) Klicken Sie auf **OK & Weiter**. Es werden Ihnen alle vorhandenen Teilnehmer-Profile und deren Mitglieder angezeigt.

9) Klicken Sie auf **OK & Weiter** und abschließend auf **Beenden**.

10.13.6 Wie Sie die Werte und Einstellungen eines Teilnehmer-Profils ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

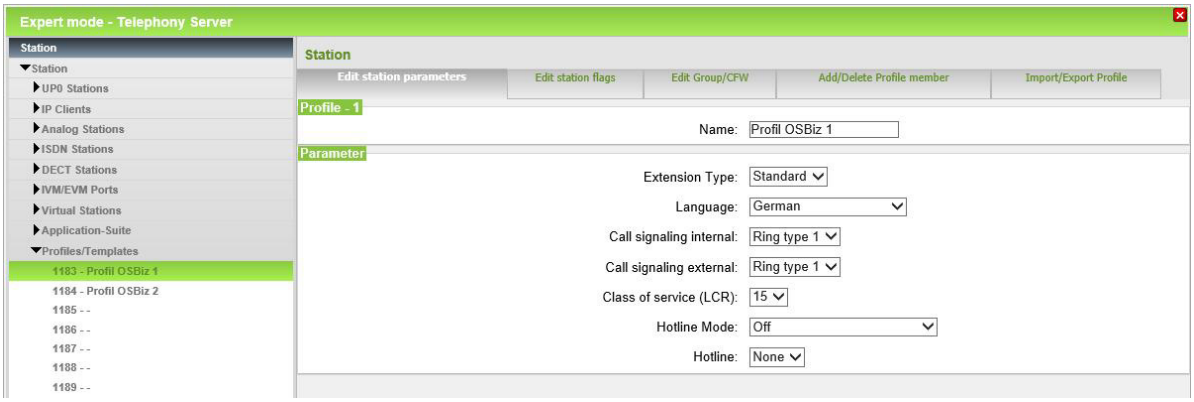
Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Teilnehmer**.

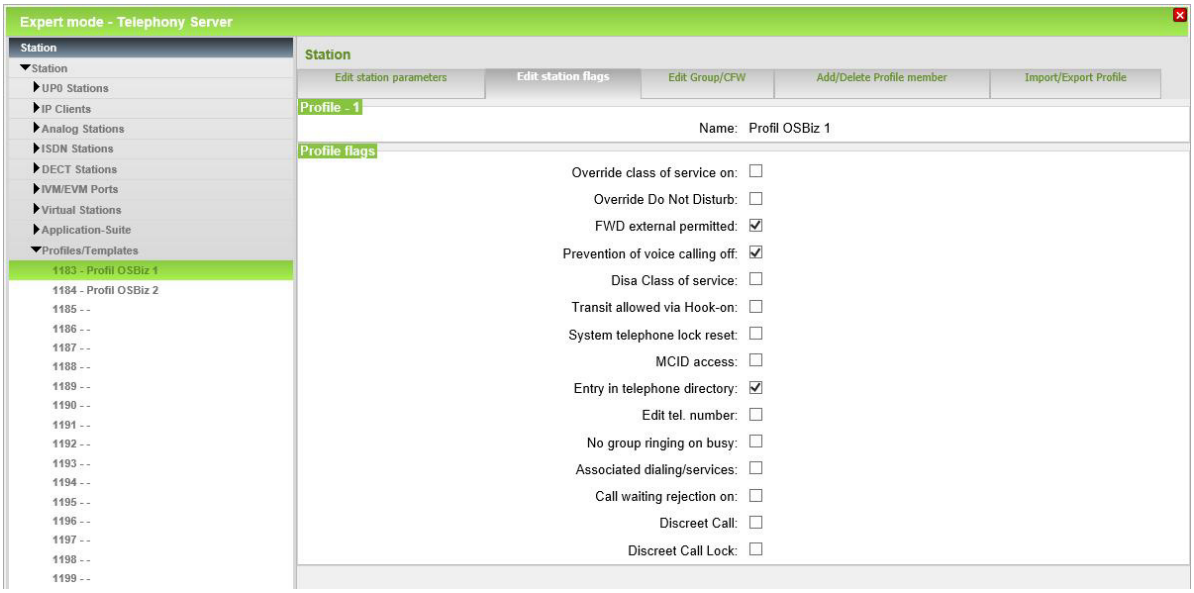
3) Klicken Sie im Menübaum auf **Teilnehmer > Profile/Templates**.

4) Klicken Sie im Menübaum auf eine Teilnehmer-Profilnummer (1156-1175).

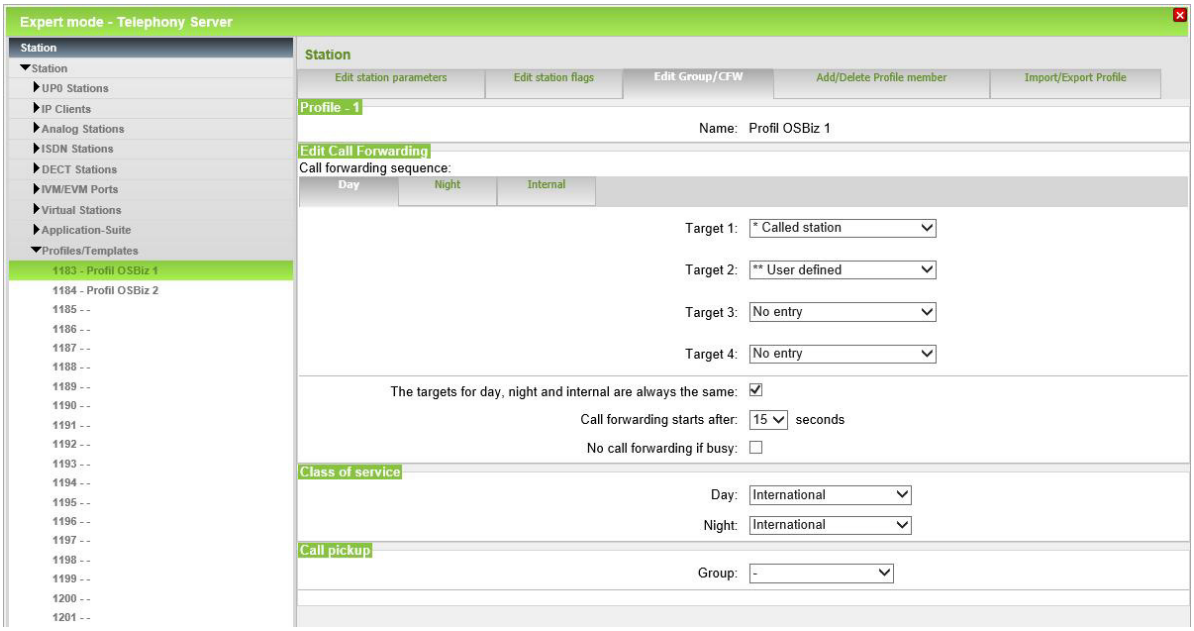


5) Ändern Sie bei Bedarf im Register **Teilnehmer-Parameter** im Feld **Name** den Namen des Teilnehmer-Profils (max. 16 Stellen möglich) und klicken Sie auf **Übernehmen**.

6) Ändern Sie bei Bedarf im Register **Teilnehmer-Parameter** die für das Teilnehmer-Profil gewünschten Teilnehmer-Parameter und klicken Sie auf **Übernehmen**.



7) Ändern Sie bei Bedarf im Register **Teilnehmer-Flags** die für das Teilnehmer-Profil gewünschten Teilnehmer-Flags und klicken Sie auf **Übernehmen**.



8) Ändern Sie bei Bedarf im Register **Gruppen/RWS** die für das Teilnehmer-Profil gewünschten Rufweiterschaltungen und klicken Sie auf **Übernehmen**.

9) Klicken Sie auf **Übernehmen**.

10.13.7 Wie Sie alle Teilnehmer-Profile exportieren oder importieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Teilnehmer**.

3) Klicken Sie im Menübaum auf **Teilnehmer > Profile/Templates**.

4) Klicken Sie auf das Register **Import/Export alle Profile**.

5) Wenn Sie alle Teilnehmer-Profile in eine Datei exportieren wollen, klicken Sie auf **Download** und speichern die Datei in einem Verzeichnis Ihrer Wahl.

6) Wenn Sie alle Teilnehmer-Profile aus einer Datei importieren wollen, klicken Sie auf **Durchsuchen**, navigieren Sie zum Ablageort der Datei und laden Sie die Datei in das Kommunikationssystem.

10.14 Konfiguration der Authentifizierungsdaten am SIP-Telefon

Die Daten für die Authentifizierung eines SIP-Teilnehmers am Kommunikationssystem sind auch am SIP-Telefon direkt einzutragen. Dazu müssen die Daten verwendet werden, die im WBM bei jedem SIP-Teilnehmer eingetragen sind.

Folgende Daten müssen aus dem WBM übernommen und am SIP-Telefon eingetragen werden (für jedes SIP-Telefon extra):

- Kennwort
  Kennwort für die Authentifizierung.
- SIP User ID / Benutzername
  Benutzername für die Authentifizierung.
- Realm
  Zone oder Domäne für die Authentifizierung.

Die Konfiguration kann über das WBM des SIP-Telefons durchgeführt werden oder direkt am Display des SIP-Telefons.

10.14.1 Wie Sie die Authentifizierungsdaten über das WBM des SIP-Telefons konfigurieren

Voraussetzungen

- Das SIP-Telefon ist ins LAN integriert.
- Der Admin-PC hat Zugang zum WBM des SIP-Telefons.
- Sie kennen die IP-Adresse des SIP-Telefons.
- Die Konfiguration ist am Beispiel eines OpenStage 60 SIP beschrieben.

Schritt für Schritt

1) Starten Sie auf dem Admin-PC den Webbrowser und rufen Sie die Anmeldeseite des WBM des SIP-Telefons auf unter folgender Adresse auf:

`https://<IP-Adresse des SIP-Telefons>`

> ***INFO:*** Lässt sich das WBM nicht starten, prüfen Sie die LAN-Verbindung und wiederholen Sie den Aufruf. Lässt es sich noch immer nicht starten, prüfen Sie, ob die IP-Adresse durch Ihre Firewall geblockt wird. Genauere Informationen finden Sie in der Dokumentation Ihrer Firewall.

2) Wenn der Webbrowser ein Problem mit einem Sicherheitszertifikat meldet, installieren Sie das Zertifikat (am Beispiel der Internet Explorers V10).

a) Schließen Sie den Webbrowser.

b) Öffnen Sie den Webbrowser mit Administratorrechten, indem Sie mit der rechten Maustaste auf das Webbrowser-Symbol klicken und im Kontextmenü den Eintrag **Als Administrator ausführen** auswählen.

c) Erlauben Sie die Benutzerkontensteuerung.

d) Rufen Sie die Anmeldeseite des WBM des SIP-Telefons unter folgender Adresse auf:

`https://<IP-Adresse des SIP-Telefons>`

e) Klicken Sie auf **Laden dieser Website fortsetzen**.

f) Klicken Sie auf die Meldung **Zertifikatsfehler** in der Navigationsleiste des Webbrowsers.

g) Klicken Sie auf **Zertifikate anzeigen**.

h) Klicken Sie auf **Zertifikat installieren** (nur sichtbar mit Administratorrechten).

i) Wählen Sie die Option **Lokaler Computer** und bestätigen Sie mit **Weiter**.

j) Wählen Sie die Option **Alle Zertifikate in folgendem Speicher speichern**, klicken Sie auf **Durchsuchen** und geben Sie **Vertrauenswürdige Stammzertifizierungsstellen** an.

k) Bestätigen Sie mit **OK** und anschließend mit **Weiter** und **Fertigstellen**.

l) Bestätigen Sie den Zertifikatimport mit **OK** und schließen Sie das Zertifikatsfenster mit **OK**.

m) Schließen Sie den Webbrowser.

n) Starten Sie den Webbrowser erneut (ohne Administratorrechte) und rufen Sie die Anmeldeseite des WBM des SIP-Telefons unter folgender Adresse auf:

`https://<IP-Adresse des SIP-Telefons>`

3) Bei der ersten Anmeldung werden aufgefordert, ein Passwort zu vergeben.

a) Geben Sie in den Feldern **Neues Passwort** und **Passwort bestätigen** ein neues Passwort ein, um das System gegen Missbrauch zu schützen. Berücksichtigen Sie Groß-/Kleinschreibung und den Zustand der Taste **Num**. Das Passwort erscheint verdeckt durch Sternchen (*).

INFO: Das Passwort muss mindestens 6 Zeichen lang sein und eine Ziffer enthalten. Bitte merken Sie sich Ihr neues Passwort genau.

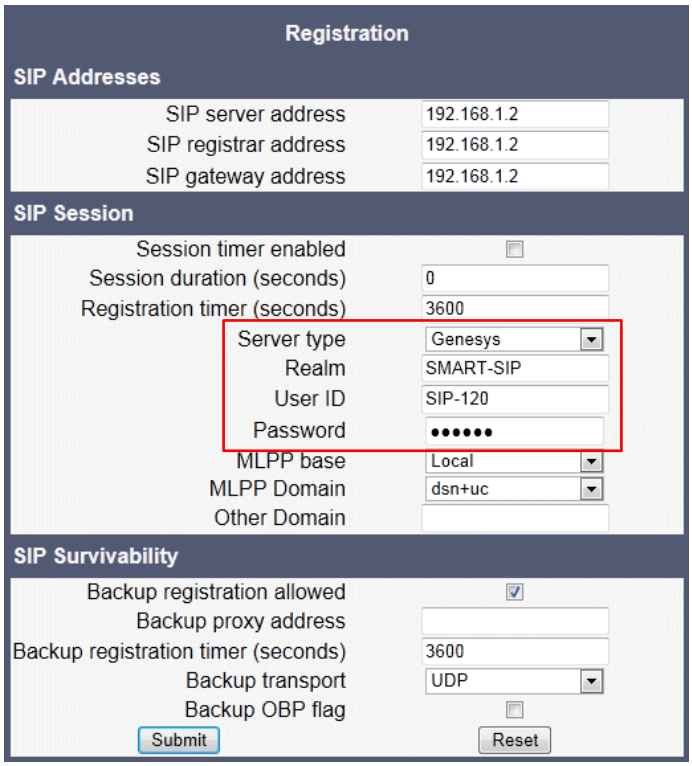
---

4) Klicken Sie auf **OK**.

5) Klicken Sie auf die Registerkarte **Administratorseiten (Admin)**.

6) Geben Sie das Administrator-Passwort ein (Standard: 123456) und klicken Sie auf **Login**..

7) Navigieren Sie zu **System > Registration**.



8) Wählen Sie im Bereich **SIP Session** aus der Aufklappliste **Server type** den Eintrag **Genesys** aus.

9) Geben Sie im Feld **Realm** den Realm-Eintrag ein, den Sie bei der SIP-Teilnehmerkonfiguration im WBM des Kommunikationssystems vergeben haben (z. B. `SMART-SIP`).

10) Geben Sie im Feld **User ID** die User ID ein, den Sie bei der SIP-Teilnehmer-konfiguration im WBM des Kommunikationssystems vergeben haben (z. B. `SIP-120`).

11) Geben Sie im Feld **Password** das Kennwort ein, den Sie bei der SIP-Teilnehmerkonfiguration im WBM des Kommunikationssystems vergeben haben.

12) Klicken Sie auf **Submit**. Die Änderungen sind gespeichert.

13) Melden Sie sich am WBM ab mit der Schaltfläche **Abmeldung**.

10.14.2 Wie Sie die Authentifizierungsdaten am Display des SIP-Telefons konfigurieren

Voraussetzungen

- Die Authentifizierungsdaten (User ID, Kennwort und Realm) sind Ihnen bekannt.
- Die Konfiguration ist am Beispiel eines OpenStage 80 SIP beschrieben.

Schritt für Schritt

1) Um in den Administrationsmodus des Systemtelefons zu gelangen, drücken Sie am Telefon die Taste für das Einstellungen-/Anwendungen-Menü.

2) Blättern Sie im Register `Einstellungen` bis `Admin` und bestätigen Sie mit der OK-Taste.

3) Geben Sie das Administrator-Passwort (Standard: `123456`) ein und bestätigen Sie mit der OK-Taste.

4) Blättern Sie bis `System` und bestätigen Sie mit der OK-Taste.

5) Blättern Sie bis `Registration` und bestätigen Sie mit der OK-Taste.

6) Blättern Sie bis `SIP session` und bestätigen Sie mit der OK-Taste.

7) Blättern Sie bis `Server type` und bestätigen Sie mit der OK-Taste.

8) Blättern Sie bis zum Eintrag `Genesys` und bestätigen Sie mit der OK-Taste.

9) Blättern Sie bis `Realm` und bestätigen Sie mit der OK-Taste.

10) Geben Sie den Realm-Eintrag ein, den Sie bei der SIP-Teilnehmerkonfiguration im WBM des Kommunikationssystems vergeben haben (z. B. `SMART-SIP`). Bestätigen Sie mit dem OK-Symbol.

11) Blättern Sie bis `User ID` und bestätigen Sie mit der OK-Taste.

12) Geben Sie die User ID ein, den Sie bei der SIP-Teilnehmerkonfiguration im WBM des Kommunikationssystems vergeben haben (z. B. `SIP-120`). Bestätigen Sie mit dem OK-Symbol.

13) Blättern Sie bis `Password` und bestätigen Sie mit der OK-Taste.

14) Geben Sie das Kennwort ein, den Sie bei der SIP-Teilnehmerkonfiguration im WBM des Kommunikationssystems vergeben haben. Bestätigen Sie mit dem OK-Symbol.

15) Bestätigen Sie die Abfrage nach der Speicherung der Änderungen, indem Sie `Save` auswählen und mit der OK-Taste bestätigen.

16) Navigieren Sie mit der Zurück-Taste zum Menü `Admin` zurück.

17) Wenn das Systemtelefon bedingt durch die Änderungen einen Neustart durchführen muss, erscheint in dem Menü `Admin` der Menüpunkt `Restart`. Bestätigen Sie `Restart` mit der OK-Taste und anschließend `Yes` ebenso mit der OK-Taste. Das Systemtelefon führt einen Neustart durch und meldet sich am Kommunikationssystem an.

10.15 Export von Teilnehmerdaten

Wichtige Teilnehmerdaten können in eine XML-Datei exportiert werden.

Zusätzlich zu den Teilnehmerdaten, wie z. B. Namen und Rufnummern der Teilnehmer, E-Mail-Adressen und Telefontyp, kann die XML-Datei weitere Daten enthalten, wie z. B. Gruppenrufnummern und Lizenzzuordnungen.

Die XML-Datei können Sie mit einem Tabellenkalkulationsprogramm wie z. B. Microsoft Office Excel bearbeiten.

Eine Vorlage mit Beispieldatensätzen und Beschreibung finden Sie in der Datei `csv-templates.zip` unter **Service-Center > Dokumente > CSV-Vorlagen**.

10.15.1 Wie Sie die Teilnehmerdaten exportieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung > Konfiguration**.

3) Klicken Sie im Menübaum auf **Konfiguration > Port-Konfiguration**.

4) Klicken Sie auf das Register **Konfiguration exportieren**.

5) Klicken Sie auf die Schaltfläche **Download**.

6) Bestätigen Sie die Abfrage mit **OK**.

7) Klicken Sie auf **Speichern** und wählen Sie den Ablageort der XML-Datei aus.

8) Klicken Sie abschließend auf **Speichern**.

11 UC Smart

UC Smart bietet die ohne UC Booster nutzbaren Unified Communications Leistungsmerkmale wie z. B. Anwesenheitsstatus und Sprachnachrichten mit dem Client myPortal for OpenStage sowie zusätzlich Konferenzen mit dem Client myPortal Smart.

Verwandte Themen

- UC-Funktionen (Überblick)

11.1 Grundeinstellungen für UC Smart

Grundlegende Einstellungen zu UC Smart können angepasst werden.

UC Smart kann aktiviert oder deaktiviert werden. Wenn UC Smart genutzt wird, muss UC Suite deaktiviert werden.

Kennwort-Einstellungen

Der Administrator muss für alle Benutzer von UC Smart ein einheitliches Initial-Kennwort vergeben und dieses Kennwort den Benutzern mitteilen. Dieses Initial-Kennwort muss der Benutzer bei seiner ersten Anmeldung an einem UC-Smart Client ändern. Ohne die Vergabe eines Initial-Kennworts kann sich der Benutzer nicht an einem UC-Smart Client anmelden.

Das vom Benutzer neu zu vergebende Kennwort sollte den strengen Kennwort-Richtlinien entsprechen.

11.1.1 Wie Sie UC Smart aktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen > Applikationsauswahl**.
3) Klicken Sie im Menübaum auf **Applikations Auswahl > Applikations Auswahl**.
4) Klicken Sie auf **Paket mit UC Smart**.
5) Klicken Sie auf **Übernehmen**.

Nächste Schritte

Wie Sie UC Smart konfigurieren

11.1.2 Wie Sie UC Smart konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.
- Im Experten-Modus ist unter **Applikationsauswahl** das **Paket mit UC Smart** aktiviert.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Smart**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **UC Smart** zu starten.

4) Klicken Sie im Menübaum auf **Administration > Grundeinstellungen**.

5) Aktivieren Sie unter **UC Smart Aktivieren / Deaktivieren** das Kontrollkästchen **Aktiv**.

6) Initial-Kennwort unter **Passwort-Policy** vergeben:

a) Klicken Sie bei **Systemweites initiales UC Smart Passwort** auf **Konfigurieren**.

b) Geben Sie im Feld **Systemweites initiales UC Smart Passwort** das Initial-Kennwort für alle UC Smart Benutzer ein.

c) Klicken Sie auf **Setzen**.

7) Kennwort-Richtlinien unter **Passwort-Policy** festlegen:

INFO: Für detaillierte Informationen zur den Kennwort-Richtlinien klicken Sie auf das Symbol **i**.

- Wenn Sie möchten, dass Benutzer-Kennwörter den strengen Kennwort-Richtlinien entsprechen müssen (empfohlen), aktivieren Sie das Kontrollkästchen **Benutzer muss sicheres Passwort eingeben**.
- Wenn Sie nicht möchten, dass Benutzer-Kennwörter den strengen Kennwort-Richtlinien entsprechen müssen (nicht empfohlen), deaktivieren Sie das Kontrollkästchen **Benutzer muss sicheres Passwort eingeben**.

8) Zugriff auf das System unter **Zugangseinstellungen** festlegen:

- Wenn Sie verschlüsselten Zugriff von UC Smart Clients auf das System aktivieren möchten (bei Nutzung von myPortal for Mobile oder myPortal to go via Internet empfohlen), aktivieren Sie das Kontrollkästchen **HTTPS**.
- Wenn Sie unverschlüsselten Zugriff von UC Smart Clients auf das System aktivieren möchten (bei Nutzung von myPortal for Mobile oder myPortal to go via Internet nicht empfohlen), aktivieren Sie das Kontrollkästchen **HTTP**.

9) Aktivieren Sie das Kontrollkästchen **Anmeldedaten im Endgerät speichern**, wenn die Anmeldedaten zusätzlich im Telefon gespeichert werden sollen.

10) Klicken Sie auf **Übernehmen**.

11.1.3 Wie Sie die IP-Adressen von Komponenten des Systems ermitteln

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Applikationen > Applikationsauswahl**.

3) Klicken Sie im Menübaum auf **Applikations Auswahl > Applikations Auswahl**.

Unter **Applikationsauswahl** werden die IP-Adressen verschiedener Komponenten des Sytrems angezeigt, z. B. von **UC Smart**, **Application Launcher**, **CSTA-Connector**, **OpenDirectory Service**, **UC Suite / XMPP**, **GateView** und **Web Collaboration**.

11.1.4 Wie Sie den Status von UC Smart ermitteln

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.
- Im Experten-Modus ist unter **Applikationsauswahl** das **Paket mit UC Smart** aktiviert.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Smart**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **UC Smart** zu starten.

4) Klicken Sie im Menübaum auf **Administration > Status**.

Unter **Applikationsserver** werden Statusinformationen zu UC Smart angezeigt, z. B. **Status**, **Version**, **Telefonanlage**, **Datenbank**, **EVM**, **Fehlende Monitorpunkte**, **Aktive Benutzer**, **Aktive Verbindungen**, **Aktive HTTPS Verbindungen**, **Mobility Entry Benutzer**, **Benutzer ohne Endgerät** und **Gesperrte Benutzer**.

11.2 UC Smart Clients

UC Smart Clients bieten Teilnehmern Oberflächen für Unified Communications.

Das System bietet folgende UC Smart Clients für folgende Geräte:

Client-Typ	Client	Gerät
Communications Client	myPortal Smart	PC
	myPortal for OpenStage (UC Smart)	OpenStage Telefon
Mobile Client	myPortal for Mobile (UC Smart) (siehe *Mobility*)	Mobiltelefon, Tablet-PC
	myPortal to go (UC Smart) (siehe *Mobility*)	Smartphone

11.2.1 myPortal Smart

myPortal Smart ist eine Adobe AIR basierte PC-Anwendung für Unified Communications für die UC-Lösung UC Smart. Neben komfortablen Wahlhilfen über Verzeichnisse und Favoriten sowie Informationen über den Anwesenheitsstatus von Kollegen haben Sie z. B. auch Zugriff auf Sprachnachrichten.

Abhängig von den Ihnen zugeordneten Lizenzen kann das Angebot der Leistungsmerkmale leicht variieren.

myPortal Smart unterstützt folgende Leistungsmerkmale:

- Anwesenheitsstatus
- Statusbezogene Anrufumleitung
- Verzeichnisse
- Favoritenliste
- Journal
- Rufnummern- und Namenssuche
- Anruffunktionen
- One Number Service
- Sprachnachrichten
- Textnachrichten

INFO: Einige Leistungsmerkmale wie Rückfrage und Konferenz stehen myPortal Smart in Verbindung mit SIP-Telefonen nicht zur Verfügung.

11.2.2 myPortal for OpenStage (UC Smart)

myPortal for OpenStage ist das Benutzerportal für den Zugriff auf Unified-Communications-Funktionen des Systems an Ihrem OpenStage-Telefon.

Die Konfiguration von myPortal for OpenStage ist über das OpenStage Telefon sowie über OpenStage Manager im Webbrowser möglich.

myPortal for OpenStage bietet folgende Leistungsmerkmale:

- Anwesenheitsstatus

11.2.3 Voraussetzungen für myPortal Smart

Um den UC Client zu nutzen muss der Client-PC eine geeignete Hardware- und Softwareausstattung haben. Für die Installation und automatische Updates sind konfigurationsabhängig Administrationsrechte erforderlich. Der nutzbare Funktionsumfang ist abhängig von den verwendeten Lizenzen.

INFO: Beachten Sie bitte unbedingt die aktuellen Informationen in Experten-Wiki.

Telefone

myPortal Smart kann in Verbindung mit folgenden Telefonen genutzt werden:

- OpenStage HFA und SIP
- OpenScape Desk Phone IP 35G/55G HFA und SIP
- OpenScape Desk Phone IP 35G Eco SIP
- OpenStage T
- SIP-Telefone mit 3PCC-Unterstützung
- Analoge Telefone
- OpenScape Personal Edition HFA und SIP
- OpenScape Business Cordless
- OpenScape Cordless IP
- optiPoint WL2 professional SIP

Ältere Geräte (z. B. optiPoint 410/420/500) werden teilweise noch unterstützt. Getestete und freigegebene Geräte entnehmen Sie bitte den jeweiligen Freigabemitteilungen.

INFO: Einige Leistungsmerkmale wie Rückfrage und Konferenz stehen myPortal Smart in Verbindung mit SIP-Telefonen nicht zur Verfügung.

INFO: Bei analogen Telefonen und DECT-Telefonen wird die Briefkastenlampe nicht unterstützt und die Anzeige von Informationen im Display nur eingeschränkt unterstützt.

Zusätzliche Software

- Adobe AIR V3.4 oder neuer

Hardware Mindestanforderungen

Entsprechend den Anforderungen von Adobe AIR.

Webbrowser

Für die Tastenprogrammierung der Telefone über den UC Client sind folgende Webbrowser freigegeben:

- Microsoft Internet Explorer Version 10 (oder neuer)
- Mozilla Firefox Version 19 (oder neuer)

Installationsdateien

Der Administrator kann die Installationsdateien aus dem **Service-Center** herunterladen und diese den Benutzern bereitstellen, z. B. über ein Netzlaufwerk.

Verwandte Themen

- Lizenzen
- Lizenzen

11.2.4 Voraussetzungen für myPortal for OpenStage (UC Smart)

Um myPortal for OpenStage zu nutzen muss das Telefon über geeignete Hardware und Software verfügen.

Die Voraussetzungen für myPortal for OpenStage (UC Smart) sind identisch zu jenen für myPortal for OpenStage (UC Suite).

Verwandte Themen

- Voraussetzungen für myPortal for OpenStage (UC Suite)

11.3 Benutzer von UC Smart

Benutzer von UC Smart sind Teilnehmer, welche UC Clients von UC Smart nutzen.

Folgende Einstellungen für UC Smart Clients sind in UC Smart Assistant verfügbar:

Einstellungen	Erklärung
Einstellungen	
Benutzer	Einstellung wird hier nur angezeigt.
Name	Einstellung wird hier nur angezeigt.
Passwort	Kennwort für UC Smart Clients und UC Smart Assistant.
Sprache	Sprache der Benutzeroberfläche.
Anwender muss neues Passwort vergeben	Einstellung wird hier nur angezeigt.
Zugriff auf UC Smart Assistant	Erlaubnis für die Nutzung von UC Smart Assistant im Webbrowser durch den Benutzer für Konfigurationsaufgaben.
Konfiguriert als Mobility-Teilnehmer	Einstellung wird hier nur angezeigt.
Voicemail-Lizenz	Einstellung wird hier nur angezeigt.
Assoziierte Dienste	Einstellung wird hier nur angezeigt.
Profildetails	
Mobile Rufnummer	Mobile Rufnummer des Teilnehmers im kanonischen Format (z. B. `+49 173 1234567`).
Private/Externe Rufnummer	Zusätzliche Rufnummer des Teilnehmers im kanonischen Format (z. B. `+49 89 987654321`).
Email-Adresse	E-Mail-Adresse des Teilnehmers.
Voicemail an Email	Aktivierung/Deaktivierung der Email-Benachrichtigung beim Eingang einer neuen Sprachnachricht.
Sichtbarkeit Präsenzstatus	Einstellung, ob der Anwesenheitsstatus für interne und externe Teilnehmer sichtbar sein soll oder nur für interne Teilnehmer oder ob er überhaupt nicht sichtbar sein soll.
Lizenzierungsinformationen	
Anzeige der dem Benutzer zugewiesenen Lizenzen	

11.3.1 Wie Sie einen Benutzer von UC Smart konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.
- Im Experten-Modus ist unter **Applikationsauswahl** das **Paket mit UC Smart** aktiviert.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards > UC Smart**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **UC Smart** zu starten.
4) Klicken Sie im Menübaum auf **Administration > Benutzerverwaltung**.
5) Wählen Sie in der Liste **Benutzer** den gewünschten Benutzer aus.
6) Geben Sie im Bereich **Einstellungen** und im Bereich **Profildetails** die Daten des Benutzers ein.
7) Klicken Sie auf **Übernehmen**.
8) Wenn Sie einen weiteren Benutzer konfigurieren möchten, wiederholen Sie die Schritte 5 bis 7.

11.3.2 Wie Sie für einen Benutzer von UC Smart das Kennwort ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.
- Im Experten-Modus ist unter **Applikationsauswahl** das **Paket mit UC Smart** aktiviert.

INFO: Bitte beachten Sie, dass UC Smart Benutzer standardmäßig ihr Passwort erneut ändern müssen, wenn der Administrator dieses geädert hat. Wenn das nicht gewünscht ist, bitte nach Ändern des Passworts das Flag "Anwender muss neues Passwort vergeben" deaktivieren.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards > UC Smart**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **UC Smart** zu starten.
4) Klicken Sie auf im Menübaum auf **Administration > Benutzerverwaltung**.
5) Wählen Sie im Bereich **Benutzer** den betreffenden Benutzer aus.
6) Geben Sie im Bereich **Einstellungen** unter **Passwort** das neue Kennwort ein.
7) Klicken Sie auf **Übernehmen**.
8) Wenn Sie das Kennwort eines weiteren Benutzers zurücksetzen möchten, wiederholen Sie die Schritte 5 bis 7.

Nächste Schritte

Informieren Sie den bzw. die betroffenen Benutzer über das neue Kennwort.

11.4 Anwesenheitsstatus (UC Smart)

Der Anwesenheitsstatus (Präsenz, Presence) informiert im internen Verzeichnis über die Verfügbarkeit interner Teilnehmer (auch Mobility-Entry-Teilnehmer). Darüber hinaus steuert der Anwesenheitsstatus die Erreichbarkeit interner Teilnehmer mit der statusbezogenen Anrufumleitung.

Sie können als Teilnehmer Ihren Anwesenheitsstatus in myPortal Smart, myPortal for Mobile, myPortal to go oder myPortal for OpenStage ändern. Bei jeder Änderung des Anwesenheitsstatus außer für **Büro** können Sie den Zeitpunkt der geplanten Rückkehr zu **Büro** festlegen.

Als Teilnehmer können Sie folgende Status auswählen:

- **Büro**
- **Besprechung**
- **Krank**
- **Pause**
- **Außer Haus**
- **Urlaub**
- **Mittagspause**
- **Zu Hause**
- **Anrufschutz**

Anrufe können über die statusbezogenen Anrufumleitung unter anderem zur persönlichen Sprachbox umgeleitet werden. Hat ein Teilnehmer keine persönliche Sprachbox, kann er Anrufe auf eine Gruppenmailbox oder eine Systemmailbox weiterleiten. Allerdings hat er via myPortal Smart keinen Zugriff auf diese Mailboxen.

11.5 Verzeichnisse und Journal (UC Smart)

Verzeichnisse und das Journal organisieren Kontakte und Anrufe.

11.5.1 Verzeichnisse (UC Smart)

Verzeichnisse organisieren die Kontakte der Teilnehmer. Teilnehmer können mit UC Smart Clients sowie mit Systemtelefonen mit Display auf Kontakte zugreifen.

Das System bietet folgende Verzeichnisse, die folgende Funktionen unterstützen:

Verzeichnis	UC Smart Clients	Systemtelefon mit Display
Persönliches Verzeichnis	Über den persönlichen Assistant importierte Outlook-Kontakte.	-
Internes Verzeichnis	Enthält alle internen Teilnehmer und Gruppen mit ihren eventuellen zusätzlichen Rufnummern, für welche das Anzeigen im System aktiviert ist. Interne Teilnehmer mit Systemtelefon werden mit Anwesenheitsstatus dargestellt. Voraussetzung für die Anzeige des Anwesenheitsstatus eines Teilnehmers ist, dass der betreffende Teilnehmer dies zulässt.	Enthält alle internen Teilnehmer und Gruppen, für welche das Anzeigen im System aktiviert ist.
Favoritenliste	Enthält vom Teilnehmer ausgewählte Kontakte aus dem persönlichen und internen Verzeichnis. Interne Teilnehmer mit Systemtelefon werden mit Anwesenheitsstatus dargestellt. Voraussetzung für die Anzeige des Anwesenheitsstatus eines Teilnehmers ist, dass der betreffende Teilnehmer dies zulässt.	-
Systemtelefonbuch	Enthält alle zentralen Kurzwahlnummern.	

INFO: Geben Sie Rufnummern in Verzeichnissen nach Möglichkeit stets im kanonischen Format ein.

11.5.1.1 Wie Sie Verzeichnisse für Systemtelefone konfigurieren (UC Smart)

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Sie können wählen, welche Verzeichnisse an Systemtelefonen mit Display zur Verfügung stehen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telephony Server > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **System > Display**.

4) Wählen Sie in der Aufklappliste **Telefonbuch** eine der folgenden Möglichkeiten:
   - Wenn sowohl das Interne Verzeichnis als auch das Externe Offline-Verzeichnis zur Verfügung stehen soll, wählen Sie **Alle**.
   - Wenn nur das Interne Verzeichnis zur Verfügung stehen soll, wählen Sie **Intern**.
   - Wenn nur das Externe Offline-Verzeichnis zur Verfügung stehen soll, wählen Sie **LDAP**.
   - Wenn kein Verzeichnis zur Verfügung stehen soll, wählen Sie **Nein**.
5) Klicken Sie auf **Übernehmen**.

Nächste Schritte

Wenn Sie **Alle** oder **LDAP** gewählt haben, sorgen Sie dafür, dass ein entsprechendes LDAP-Verzeichnis für Systemtelefone zur Verfügung steht.

11.5.2 Internes Verzeichnis (UC Smart)

Das interne Verzeichnis enthält die Kontaktdetails der internen Teilnehmer und der Gruppen des Kommunikationssystems. UC Smart Clients haben Zugriff auf das interne Verzeichnis.

Als Administrator haben Sie uneingeschränkten Zugriff auf alle Daten im internen Verzeichnis. Als Teilnehmer können Sie aus dem internen Verzeichnis wählen.

Verwandte Themen

- Gruppenruf
- Sammelanschluss

11.5.2.1 Wie Sie die Anzeige eines Teilnehmers im internen Verzeichnis aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Teilnehmer**.
3) Navigieren Sie im Menübaum unter **Teilnehmer > Teilnehmer > ...** zum gewünschten Teilnehmer (Index-Rufnummer-Name).
4) Klicken Sie auf die Registerkarte **Teilnehmer-Flags ändern**.

5) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn der Name des Teilnehmers im internen Verzeichnis angezeigt werden soll, aktivieren Sie das Kontrollkästchen **Eintrag in Telefonbuch**.
- Wenn der Name des Teilnehmers nicht im internen Verzeichnis angezeigt werden soll, deaktivieren Sie das Kontrollkästchen **Eintrag in Telefonbuch**.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

11.5.3 Favoritenliste (UC Smart)

Die Favoritenliste enthält die vom Teilnehmer ausgewählten Kontakte aus dem persönlichen und internen Verzeichnis. UC Smart Clients haben Zugriff auf die Favoritenliste.

Ein UC Smart Benutzer kann aus der Favoritenliste direkt einen Kontakt anrufen. Erhält ein interner Teilnehmer einen Anruf, wird das im Anwesenheitsstatus des Teilnehmers angezeigt. Der UC Smart Benutzer kann diesen Anruf übernehmen.

11.5.4 Systemtelefonbuch (UC Smart)

Das Systemtelefonbuch enthält alle zentralen Kurzwahlnummern für welche jeweils ein Name vergeben wurde. UC Smart Clients haben Zugriff auf das Systemtelefonbuch.

Der Administrator kann die Anzeige für jeden Teilnehmer bzw. jede Kurzwahlnummer mit Namen individuell deaktivieren.

11.5.5 Journal (UC Smart)

Das Journal ist die Liste aller ankommenden und gehenden Anrufe eines Teilnehmers. Aus dem Journal kann der Teilnehmer Kontakte schnell und einfach erneut anrufen oder entgangene Anrufe beantworten.

Ordner für Anrufarten

Die Anrufe können in folgende Gruppen gegliedert sein:

- **Alle Anrufe**
- **Entgangen**
- **Angenommen**
- **Ankommend**
- **Gehend**

Gruppierung nach Zeitraum

Die Anrufe sind in jeder Gruppe zeitlich gruppiert, z. B.: Heute, Gestern, etc., Letzte Woche, Letzten Monat und Älter. Ihr Administrator kann einstellen, wie lange Anrufe im Journal gespeichert bleiben. Nach der eingestellten Zeit werden Einträge automatisch gelöscht.

Anrufdetails

Jeder Anruf wird mit Datum und Uhrzeit angezeigt und sofern vorhanden mit der Rufnummer. Falls ein Verzeichnis zur Rufnummer weitere Informationen enthält wie **Nachname** und **Vorname**, werden auch diese angezeigt. Zusätzlich angezeigt wird in den meisten Ordnern die **Richtung** des Anrufs und bei myPortal Smart auch **Dauer**.

11.6 Anrufe (UC Smart)

Für Anrufe ist das Rufnummernformat von besonderer Bedeutung.

11.6.1 Rufnummernformate

Für die Angabe von Rufnummern existieren unterschiedliche Formate.

Format	Beschreibung	Beispiel
kanonisch	Beginnt mit + und enthält stets Landeskennzahl, Ortskennzahl und die komplette restliche Rufnummer. Leerzeichen und die Sonderzeichen + ( ) / - : ; sind zulässig.	+49 (89) 7007-98765
wählbar	So, wie Sie die Rufnummer am Systemtelefon im Büro wählen würden, stets mit Amtskennzahl.	• 321 (intern) • 0700798765 (eigenes Ortsnetz) • 0089700798765 (fremdes Ortsnetz) • 0004989700798765 (Ausland)

INFO: Verwenden Sie wo immer möglich das kanonische Rufnummernformat. Damit ist eine Rufnummer in jeder Situation vollständig und eindeutig und auch bei Vernetzung konsistent.

Bei der manuellen Wahl (wählbares Format) einer externen Rufnummer muss die Amtskennzahl immer mitgewählt werden. Auch bei der manuellen Eingabe der Zielrufnummer (wählbares Format) für den CallMe-Dienst (UC Suite) in UC Clients muss die Amtskennzahl mit eingegeben werden.

Bei der Wahl einer externen Rufnummer im wählbaren Format aus einem Verzeichnis (sowie mit bestimmten UC Clients bei Desktop-Wahl und Clipboard-

Wahl) ergänzt das Kommunikationssystem die Amtskennzahl automatisch (Richtung 1). Die automatische Ergänzung der Amtskennzahl erfolgt auch, wenn als Zielrufnummer für den CallMe-Dienst (UC Suite) eine Rufnummer der eigenen persönlichen Daten ausgewählt wird (**Mobilrufnummer**, **private Rufnummer**, etc.).

INFO: Bei Anrufen innerhalb der USA über CSTA zu einer Rufnummer im kanonischen Format wird die Rufnummer in das wählbare Format konvertiert.

11.7 Konferenzen (UC Smart)

In einer Konferenz können mehrere Teilnehmer (darunter auch externe) gleichzeitig miteinander telefonieren.

11.7.1 Ad-hoc-Konferenz (UC Smart)

Eine Ad-hoc-Konferenz (telefongesteuert) findet spontan statt. Der Konferenzleiter startet sie manuell.

Interne Teilnehmer können eine Konferenz initiieren. Der Initiator einer Konferenz ist der Konferenzleiter. Er kann Konferenzteilnehmer aus der Konferenz herausschalten oder die Konferenz vollständig auflösen. Außerdem kann er sich aus der Konferenz herausschalten, ohne dass die Konferenz beendet wird. Verbleiben noch interne Teilnehmer in der Konferenz, so ist der neue Konferenzleiter jener interne Teilnehmer, der am längsten an der Konferenz teilgenommen hat. Legt der neue Konferenzleiter auf, entscheidet dessen Teilnehmer-Flag “Transit schalten durch Auflegen“ über den weiteren Verlauf der Konferenz: Ist dieses Flag nicht gesetzt, wird die Konferenz beendet. Verbleiben nur externe Teilnehmer in der Konferenz und ist kein Rückwärtsauslösekriterium vorhanden, (z. B. analoges Amt), wird der Timer "Zeit bis zum Aufmerksamkeitston bei HKZ-Transit-Verbindungen" gestartet (einstellbar von 0 bis 255 Minuten, Default-Einstellung = 5 Minuten). Nach Ablauf dieses Timers erhalten die verbleibenden Teilnehmer einen Warnton und der Timer "Zeit vom Aufmerksamkeitston bis zum Auslösen ..." wird gestartet (einstellbar von 0 bis 10 Minuten, Default-Einstellung = 10 Sekunden). Nach Ablauf dieses Timers wird die Konferenz vom System beendet.

Teilnehmer der Konferenz können diese verlassen, indem sie auflegen oder einen zweiten Anruf annehmen. Sie müssen jedoch den Konferenzleiter anrufen, um wieder an der Konferenz teilzunehmen.

Silent Monitoring

Silent Monitoring schränkt die maximale Anzahl von Konferenzen eint. Die maximale Anzahl von Konferenzen entspricht der maximalen Anzahl gleichzeitiger Silent Monitoring-Teilnehmer.

11.8 Sprachbox / SmartVM (UC Smart)

Die Sprachbox (auch SmartVM genannt) spielt Anrufern eine Begrüßung vor und bietet ihnen die Möglichkeit, eine Nachricht aufzusprechen oder sich weitervermitteln zu lassen. Interne Teilnehmer können über ein Telefon und mit dem UC Smart Client myPortal Smart auf die Sprachbox zugreifen. Teilnehmer, die eine Sprachbox nutzen wollen, benötigen eine VoiceMail-Lizenz.

Sprachbox-Typen

Es gibt folgende Sprachbox-Typen:

- Standardmailbox:
  Die Standardmailbox ist die persönliche Sprachbox eines Teilnehmers. Sie nimmt den Anruf entgegen, begrüßt den Anrufer mit einer persönlichen Ansage oder einer Standardansage und bietet dem Anrufer die Möglichkeit eine Nachricht aufzusprechen. Die Standard-Mailbox wird vom Teilnehmer über das Telefon oder über myPortal Smart konfiguriert (z. B. Aufsprechen einer persönlichen Begrüßung).
- Gruppenmailbox:
  Die Gruppenmailbox hat die gleichen Eigenschaften wie die Standardmailbox, nur dass sie nicht einem einzelnen Teilnehmer zugeordnet ist, sondern einer Gruppe von Teilnehmern. Nachrichten können für eine Gruppenmailbox nur aufgezeichnet werden, wenn mindestens ein Gruppenmitglied eine VoiceMail-Lizenz besitzt. Die Info der Sprachbox wird allen Gruppenmitgliedern mit einer VoiceMail-Lizenz angezeigt. Das Abhören der Nachrichten ist über das Telefonmenü der persönlichen Sprachbox der Gruppenmitglieder möglich.
- Vermittlungsmailbox (AutoAttendant / Company AutoAttendant):
  Die Vermittlungsmailbox bietet Anrufern eine Begrüßung mit oder ohne anschließender Vermittlungsmöglichkeit. Eine spezielle Form der Vermittlungsmailbox ist der Company AutoAttendant. Hier kann der Anrufer automatisch weitergeleitet werden (z. B. zur Vermittlung) oder durch Wahl einer internen Rufnummer oder Kurzwahlnummer (Ziffern 0-9) zu einem Teilnehmer weitergeleitet werden (z. B. zum Service oder zur Hotline). Natürlich muss eine entsprechende Ansage diese Wahlmöglichkeiten erläutern. Außerdem kann ein Abwurfziel eingerichtet werden, zu dem der Anrufer weitergeleitet wird, wenn er keine Ziffer oder eine falsche (nicht belegte) Ziffer drückt. Der Administrator kann bis zu 100 Vermittlungsmailboxen konfigurieren.
- Ansagemailbox:
  Durch Zuweisen eines Ansagenindex zu einem Ansageport und Konfiguration einer Mailbox mit der Rufnummer des Ansageports wird die Ansagefunktion konfiguriert. Als Ansage wird die Begrüßung der Mailbox verwendet.

Die Wiedergabe kann je nach eingestelltem Ansagetyp einmalig erfolgen (Ansage) oder zyklisch (Musik). Das Telefonmenü einer Ansagemailbox kann nur von einem anderen Telefon aus benutzt werden, da kein zugehöriges Telefon existiert. Daher muss für die Ansagemailbox eine andere PIN verwendet werden als für die Sprachbox des benutzten Telefons.

- Systemmailbox:
  Als Systemmailbox wird die Sprachmailbox mit der Rufnummer des Sammelanschlusses der SmartVM benutzt. Die Systemmailbox muss eine Standardmailbox (kein AutoAttendant) mit aktivierter Sprachaufzeichnung sein. Die Info der Sprachbox wird dem Besitzer der Sprachbox mit dem Index 1 angezeigt und kann dort auch abgefragt werden. Diese erste Sprachbox sollte keine Gruppenmailbox, Vermittlungsmailbox oder Ansagemailbox ein. Soll die Systemmailbox nicht genutzt werden, sollte keine Sprachmailbox mit der Rufnummer des SmartVM Sammelanschlusses eingerichtet werden.

Funktionen der Sprachbox

- Telefonische Abfrage und Steuerung
  (von extern: eine eigene Rufnummer erforderlich)
- Manuelle oder automatische Auswahl unterschiedlicher Begrüßungen
- Telefonmenü (Telephone User Interface, TUI) mit systemweit umschaltbarer Menüstruktur:
  - Telefonmenü UC Smart: **SmartVM** (ähnlich Xpressions Compact / EVM)
  - Telefonmenü UC Suite: **OSO** (ähnlich UC Suite)
- Bis zu 320 Sprachboxen pro System einrichtbar
- Bis zu 32 Stunden Sprachaufzeichnungskapazität pro System
- Bis zu 100 abgespeicherte Nachrichten pro Sprachbox
- Bis zu 2 min Aufzeichnungsdauer einer Sprachnachricht pro Sprachbox
- Bis zu 10 gleichzeitig mögliche Vermittlungs- und Anrufbeantwortervorgänge
- Ansage/Musikeinspielung vor dem Melden
- Abspielen individueller Ansagen
- Weiterleitung von Faxanrufen durch automatische Faxtonerkennung an ein vorkonfiguriertes Faxziel

> ***INFO:*** Informationen zum Telefonmenü finden Sie in den beiden Kurzbedienungsanleitungen UC Smart Telephone User Interface (TUI) und UC Suite Telephone User Interface (TUI).

Codenummer-Einstellungen

Vor der ersten Benutzung der Sprachbox muss jeder Teilnehmer die vorbelegte Codenummer ändern (Standard: `123456`).

Die Codenummer besteht aus einer sechsstelligen Ziffernfolge. Sie darf nicht aus sich wiederholenden Ziffern (z. B. `333333`) oder einer auf- bzw. absteigendenden Ziffernfolge (z. B. `987654`) bestehen. Nach sechsmaliger Eingabe einer falschen Codenummer wird der Zugriff auf die entsprechende Sprachbox bis zum

Rücksetzen des Kennworts durch den Administrator gesperrt. Nach zweimaliger Eingabe eines falschen Kennworts im Telefonmenü wird die Verbindung getrennt.

Ports

Die Sprachbox nutzt die S_0-Ports 500-509 mit den jeweils zugeordneten Rufnummern 739-748. Die Ports 504 und 505 sind standardmäßig dem Company AutoAttendant (Rufnummer 352) zugeordnet, die restlichen 8 Ports dem Sprachbox-Sammelanschluss (Rufnummer 351). Die Rufnummer 351 ist die allgemeine Rufnummer der Sprachbox, über die das Telefonmenü erreichbar ist.

Amtsberechtigung

Die Sprachbox-Ports sind aus Sicherheitsgründen standardmäßig nur halbamtsberechtigt. Folgende Leistungsmerkmale erfordern die Zuweisung einer amtsberechtigten Berechtigungsgruppe:

- Absender einer Sprachnachricht anrufen
- Abhören von Sprachnachrichten durch Mobility-Teilnehmer via Rückruf
- Übergeben zu externem Ziel durch Company AutoAttendant

Begrüßungen/Ansagen

Individuelle Begrüßungen (=Ansagen) werden entweder über ein Telefon aufgesprochen oder mit dem WBM in das System geladen. Bei der Konfiguration über das Telefon wird die Sprachbox-Rufnummer gewählt und mit Hilfe der Benutzerführung der Sprachbox kann eine neue Begrüßung über das Telefon aufgesprochen werden.

Begrüßungen können aber auch über den Experten-Modus für jede Sprachbox separat in das System geladen, gespeichert und gelöscht werden.

11.8.1 Konfiguration der Sprachbox / SmartVM

Die Konfiguration der Sprachbox (SmartVM) beinhaltet die Konfiguration der Standardmailboxen/Gruppenmailboxen und der Vermittlungsmailboxen.

Allgemeine Einstellungen zur Sprachbox (SmartVM) werden über den Wizard **SmartVM** durchgeführt, wie z. B. die Anpassung der Sprachbox-Rufnummer an einen 4-stelligen Rufnummernplan.

Spezielle Einstellungen zur Sprachbox (SmartVM) und die Einrichtung von Standardmailboxen/Gruppenmailboxen und Vermittlungsmailboxen werden über den Experten-Modus durchgeführt.

> ***INFO:*** Das Ändern einer Rufnummer setzt die Sprachbox des betreffenden Teilnehmers zurück. Alle persönlichen Sprachnachrichten, Begrüßungen und Ansagen gehen verloren und das Kennwort wird zurückgesetzt.

Sie können auch einzelne Bergüßungen in die SmartVM laden, speichern und löschen sowie Begrüßungen und Nachrichten einzelner oder aller Sprachboxen

sichern und wiederherstellen. Zusätzlich können Sie die geladenen Sprachen der Benutzerführung abfragen und sich die 10 Sprachboxen mit den meisten Nachrichten sowie den von Nachrichten und Begrüßungen belegten Speicherplatz anzeigen lassen.

Die Einrichtung von Vermittlungsmailboxen finden Sie im Kapitel Attendants - AutoAttendants - Company AutoAttendant (UC Smart).

Zuordnung der Mailbox zu den Teilnehmern

Ist die Sprachbox (SmartVM) konfiguriert, können den Teilnehmern ihre Standardmailboxen zugeordnet werden. Das ist möglich über

- eine Rufweiterschaltung für den Teilnehmer mit Hilfe einer Rufzielliste (wird vom Administrator eingerichtet). In diesem Fall wird der Anruf der Reihe nach an die ausgewählten Rufziele weitergeleitet (z. B. zuerst an den Teilnehmer und nach einer einstellbaren Zeit an die Mailbox).
- eine Anrufumleitung am Telefon des Teilnehmers (kann der Teilnehmer selbst ausführen). In diesem Fall geht der Anruf sofort an die Mailbox.
  Ist der Teilnehmer Mitglied eines Sammelanschlusses und wird der Sammelanschluss angerufen, wird der Anruf nicht auf die Sprachbox des Sammelanschlusses umgeleitet.

11.8.1.1 Wie Sie die Sprachbox deaktivieren oder aktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.
- UC Smart ist aktiviert.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telephonie > Anschaltungen**.

3) Klicken Sie im Menübaum auf **Anschaltungen > SmartVM**.

4) Klicken Sie auf die Registerkarte **SmartVM-Parameter bearbeiten**.

5) Wenn Sie die Sprachbox deaktivieren möchten, aktivieren Sie das Kontrollkästchen **EVM deaktivieren**.

6) Wenn Sie die Sprachbox aktivieren möchten, deaktivieren Sie das Kontrollkästchen **EVM deaktivieren**.

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

11.8.1.2 Wie Sie die Sprachbox / SmartVM konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Zentrale Telefonie**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **SmartVM** zu starten.

4) Aktivieren Sie das Kontrollkästchen **SmartVM aktivieren**.

5) Ändern Sie bei Bedarf die allgemeinen Einstellungen der Systemmailbox unter der Spalte **Voicemail**:

- ***a)*** Ändern Sie bei Bedarf im Feld **Rufnummer** die Rufnummer der Sprachbox (Standard: `351`), um sie z. B. an einen 4-stelligen Rufnummernplan anzupassen.
- ***b)*** Ändern Sie bei Bedarf im Feld **DuWa** die Durchwahlnummer der Sprachbox (Standard: `351`), um sie z. B. an einen 4-stelligen Rufnummernplan anzupassen.
- ***c)*** Ändern Sie bei Bedarf im Feld **Name** den Namen der Sprachbox (Standard: `VOICEMAIL`).

6) Ändern Sie bei Bedarf die allgemeinen Einstellungen für die Vermittlungsmailbox unter der Spalte **AutoAttendant**:

- ***a)*** Ändern Sie bei Bedarf im Feld **Rufnummer** die Rufnummer der Sprachbox (Standard: `352`), um sie z. B. an einen 4-stelligen Rufnummernplan anzupassen.
- ***b)*** Ändern Sie bei Bedarf im Feld **DuWa** die Durchwahlnummer der Sprachbox (Standard: `352`), um sie z. B. an einen 4-stelligen Rufnummernplan anzupassen.
- ***c)*** Ändern Sie bei Bedarf im Feld **Name** den Namen der Sprachbox (Standard: `AutoAttendant`).

7) Klicken Sie auf **OK & Weiter**.

8) Ändern Sie in der Zeile des gewünschten Ports bei Bedarf im Feld **Rufnr.** die Rufnummer des Ports (Standard: `739-748`), um sie z. B. an einen 4-stelligen Rufnummernplan anzupassen.

9) Ändern Sie in der Zeile des gewünschten Ports bei Bedarf im Feld **Name** den Namen des Ports (Standard: `SmartVM 1-10`).

10) Ändern Sie in der Zeile des gewünschten Ports bei Bedarf in der Aufklappliste **Typ** den Typ des Ports:

- **Phone Mail (Ruf-Nr. 5-stellig)**: der Port ist den Standardmailboxen und den Vermittlungsmailboxen vom Typ AutoAttendant zugeordnet. Ports dieses Typs werden automatisch in den Sammelanschluss 351 aufgenommen.
- **Standard**: der Port ist den Vermittlungsmailboxen vom Typ Company AutoAttendant und den Ansagemailboxen zugeordnet. Ports dieses Typs werden automatisch in den Sammelanschluss 352 aufgenommen.

11) Ändern Sie in der Zeile des gewünschten Ports bei Bedarf in der Aufklappliste **Modus** den Modus des Ports:

- **Ansage**: eine Begrüßung/Ansage wird einmalig abgespielt.
- **Wartemusik**: Begrüßung/Ansage/Musik wird in einer Endlosschleife abgespielt.
- **Company AutoAttendant**: nach Abspielen einer Begrüßung/Ansage besteht die Möglichkeit der Weitervermittlung.

12) Klicken Sie auf **OK & Weiter**.

13) Wählen Sie in der Aufklappliste **Mailbox-Auswahl** die gewünschte Mailbox aus. Anschließend erscheinen Felder für die Konfiguration der Begrüßungen.

14) Wenn Sie eigene Begrüßungen für die ausgewählte Mailbox verwenden wollen, klicken Sie auf **Durchsuchen**, navigieren Sie zum Ablageort der Dateien (Format: wave, PCM, 16 bit, 8kHz, mono) und klicken Sie auf **Laden**. Die ausgewählten Begrüßungen werden in das System geladen.

INFO: Bereits geladene Begrüßungen können Sie speichern und löschen.

---

15) Wenn Sie Begrüßungen für weitere Mailboxen einrichten möchten, wiederholen Sie die 13 Schritte bis 14.

16) Klicken Sie auf **OK & Weiter**.

17) Ändern Sie die allgemeinen Parameter nur bei Bedarf. Für eine Beschreibung der allgemeinen Parameter siehe *Anschaltungen > SmartVM*.

18) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

11.8.1.3 Wie Sie eine Standardmailbox für einen Teilnehmer hinzufügen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.
- Dem entsprechenden Teilnehmer ist eine Voicemail-Lizenz zugeordnet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telephonie > Anschaltungen**.

3) Klicken Sie im Menübaum auf **Anschaltungen > SmartVM**.

4) Klicken Sie auf die Registerkarte **SmartVM-Mailboxen bearbeiten**.

5) Geben Sie im Feld **Mailbox-Rufnummer** die Rufnummer des Teilnehmers ein, für den die Mailbox hinzugefügt werden soll.

6) Wählen Sie aus der Aufklappliste **Begrüßung** eine Begrüßung aus.

7) Wenn ein Anrufer eine Nachricht auf der Sprachbox hinterlassen darf, aktivieren Sie das Kontrollkästchen **Aufnahme**.

8) Vergewissern Sie sich, dass das Kontrollkästchen **AutoAttendant** deaktiviert ist.

9) Das Kontrollkästchen **Passwort Reset** muss bei einer Neueinrichtung einer Sprachbox nicht gesetzt sein. Es bewirkt das Rücksetzen des Kennworts der Sprachbox. Bei einer Neueinrichtung muss der Teilnehmer sowieso beim ersten Zugriff auf seine Sprachbox das Initial-Kennwort ändern.

10) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

11.8.1.4 Wie Sie die Berechtigungsgruppe für einen Sprachbox-Port ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.
- UC Smart ist aktiviert.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telephonie > Berechtigungen**.

3) Klicken Sie im Menübaum auf **Berechtigungen > Teilnehmer > IVM/EVM Ports > EVM** und anschließend auf den gewünschten Sprachbox-Port.

4) Wählen Sie in der Registerkarte **Berechtigungsgruppe ändern** aus den Aufklapplisten **Berechtigungsgruppe Tag** und **Berechtigungsgruppe Nacht** die gewünschte Berechtigungsgruppe für Tagbetrieb und Nachtbetrieb aus.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

11.8.1.5 Wie Sie die Struktur des Telefonmenüs der Sprachbox ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.
- UC Smart ist aktiviert.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telephonie > Anschaltungen**.

3) Klicken Sie im Menübaum auf **Anschaltungen > SmartVM**.

4) Klicken Sie auf die Registerkarte **SmartVM-Parameter bearbeiten**.

5) Wenn Sie die Struktur des Telefonmenüs der Sprachbox ähnlich zur Xpressions Compact sein soll, wählen Sie in der Aufklappliste **Telephone User Interface (TUI)** den Eintrag **SmartVM** aus.

6) Wenn Sie die Struktur des Telefonmenüs der Sprachbox ähnlich zur OpenScape Office sein soll, wählen Sie in der Aufklappliste **Telephone User Interface (TUI)** den Eintrag **OSO** aus.

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

11.8.1.6 Wie Sie einzelne Begrüßungen laden, sichern und löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.
- UC Smart ist aktiviert.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung > Konfiguration**.

3) Klicken Sie im Menübaum auf **Konfiguration > SmartVM Configuration > Dateioperationen**.

4) Klicken Sie auf die Registerkarte **Begrüßungsansagen**.

5) Wählen Sie aus der Aufklappliste **Mailbox-Auswahl** die gewünschte Sprachbox aus.

6) Wenn Sie eine zuvor gespeicherte Begrüßung oder eine Wave-Datei in die SmartVM laden wollen, klicken Sie bei der gewünschten Begrüßung auf **Durchsuchen** und navigieren Sie zum Ablageort der Begrüßung. Klicken Sie anschließend auf **Laden**.

> ***INFO:*** Die zu ladende Wave-Datei muss folgendes Format haben: PCM, 16 bit, 8khz, mono. Beim Laden wird die Wave-Datei konvertiert. Je nach Größe der Wave-Datei kann dies einige Zeit in Anspruch nehmen.

7) Wenn Sie eine bestehende Begrüßung sichern wollen, klicken Sie bei der gewünschten Begrüßung auf **Sichern** und speichern Sie die vma-Datei an einem Ort Ihrer Wahl.

8) Wenn Sie eine bestehende Begrüßung löschen wollen, klicken Sie bei der gewünschten Begrüßung auf **Löschen** und bestätigen Sie mit **OK**.

11.8.1.7 Wie Sie Begrüßungen und Nachrichten sichern und wiederherstellen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.
- UC Smart ist aktiviert.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung > Konfiguration**.

3) Klicken Sie im Menübaum auf **Konfiguration > SmartVM Configuration > Dateioperationen**.

4) Wenn Sie Begrüßungen und Nachrichten sichern wollen:

a) Klicken Sie auf die Registerkarte **Backup**.

b) Aktivieren Sie das Kontrollkästchen **Nachrichten**, wenn zusätzlich zu den Begrüßungen auch die Nachrichten gesichert werden sollen.

c) Übernehmen Sie die zu sichernden Sprachboxen aus der Liste **Verfügbare Mailboxen** in die Liste **Zu sichernde Mailboxen**.

d) Klicken Sie auf **Übernehmen**. Die Begrüßungen (und die Nachrichten, wenn Flag **Messages** aktiviert wurde) der zu sichernden Sprachboxen werden in eine Sicherungsdatei (*.tar) gesichert. Speichern Sie die Datei an einem Ort Ihrer Wahl.

5) Wenn Sie Begrüßungen und Nachrichten wiederherstellen wollen:

a) Klicken Sie auf die Registerkarte **Restore**.

b) Klicken Sie auf **Durchsuchen** und navigieren Sie zum Ablageort Ihrer Sicherungsdatei (*.tar) und klicken Sie auf **Öffnen**.

c) Klicken Sie auf **Laden** und auf **OK**. Die in der Sicherungsdatei enthaltenen Sprachboxen werden angezeigt.

d) Übernehmen Sie die wiederherzustellenden Sprachboxen aus der Liste **Verfügbare Mailboxen** in die Liste **Wiederherzustellende Mailboxen**.

e) Aktivieren Sie das Kontrollkästchen **Nachrichten**, wenn nicht nur die Begrüßungen der ausgewählten Sprachboxen, sondern auch die Nachrichten wiederhergestellt werden sollen.

f) Ist das Kontrollkästchen **Aufschalten** deaktiviert, werden nur die Begrüßungen der ausgewählten Sprachboxen überschrieben, die in den Sicherungsdaten vorhandenen sind. Ist zusätzlich das Kontrollkästchen **Nachrichten** aktiviert, werden auch die in den Sicherungsdaten enthaltenen Nachrichten hinzugefügt. Die bereits existierenden Nachrichten bleiben erhalten

g) Ist Kontrollkästchen **Aufschalten** aktiviert, werden vor der Wiederherstellung alle Begrüßungen und Nachrichten der ausgewählten Sprachboxen in der SmartVM gelöscht. Sind Sprachboxen ausgewählt, die nicht in den Sicherungsdaten enthaltenen sind, werden diese auch gelöscht! Die in den Sicherungsdaten enthaltenen Begrüßungen werden übertragen. Ist zusätzlich das Kontrollkästchen **Nachrichten** aktiviert, werden auch die in den Sicherungsdaten enthaltenen Nachrichten übertragen.

h) Klicken Sie auf **Laden** und auf **OK**. Die Begrüßungen und Nachrichten der ausgewählten Sprachboxen wieder hergestellt.

11.8.2 Benachrichtigungsdienst für neue Nachrichten

Das System kann einen UC Smart Benutzer über eine neue Sprachnachricht auf Wunsch per E-Mail informieren.

Voraussetzung für den Benachrichtigungsdienst

- Der E-Mail-Versand (E-Mail-Weiterleitung) muss im System vom Administrator konfiguriert sein.
- Die E-Mail-Adresse des Benutzers muss dem System bekannt sein. Der Administrator kann alle E-Mail-Adressen im WBM während der Erstinstallation über eine XML-Datei importieren oder im UC Smart Assistant für jeden Benutzer eine E-Mail-Adresse eintragen (siehe *Wie Sie einen Benutzer von UC Smart konfigurieren*). Alternativ kann der Benutzer selbst seine E-Mail-Adresse in seinem UC Smart Client angeben.
- Dem Benutzer ist eine VoiceMail-Lizenz zugewiesen.
- Das Leistungsmerkmal Voicemail an Email ist aktiviert. Der Administrator kann das Leistungsmerkmal im UC Smart Assistant für jeden Benutzer aktivieren (*Wie Sie die E-Mail-Benachrichtigung aktivieren oder deaktivieren*). Alternativ kann der Benutzer selbst das Leistungsmerkmal in seinem UC Smart Client aktivieren.

Der UC Smart Benutzer erhält eine E-Mail mit der Sprachnachricht als angehängte WAV-Datei (16 bit, mono), Datum und Uhrzeit des Empfangs, Dauer der Sprachnachricht und sofern verfügbar Rufnummer sowie Name des Absenders.

11.8.2.1 Wie Sie die E-Mail-Benachrichtigung aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.
- Im Experten-Modus ist unter **Applikationsauswahl** das **Paket mit UC Smart** aktiviert.
- Die E-Mail-Adresse des Benutzers ist in seinen Profildetails eingetragen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Smart**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **UC Smart** zu starten.

4) Klicken Sie im Menübaum auf **Administration > Benutzerverwaltung**.

5) Wählen Sie in der Liste **Benutzer** den gewünschten Benutzer aus.

6) Wählen Sie eine der folgenden Möglichkeiten:

a) Wenn Sie den Benachrichtigungsdienst für neue Nachrichten aktivieren wollen, aktivieren Sie im Bereich **Profildetails** das Kontrollkästchen **Voicemail an Email**.

b) Wenn Sie den Benachrichtigungsdienst für neue Nachrichten deaktivieren wollen, deaktivieren Sie im Bereich **Profildetails** das Kontrollkästchen **Voicemail an Email**.

7) Klicken Sie auf **Übernehmen**.

8) Wenn Sie einen weiteren Benutzer konfigurieren möchten, wiederholen Sie die Schritte 5 bis 7.

11.9 Instant Messaging (UC Smart)

Instant Messaging ist die Kommunikation mittels Sofortnachrichten (Chat).

11.9.1 Sofortnachrichten

Mittels Sofortnachrichten können Sie mit anderen Benutzern von UC Smart chatten.

Gesendete und empfangene Sofortnachrichten werden bei den Kommunikationspartnern als Dialog angezeigt. Beim Auswählen eines Empfängers zeigt der Client an, ob der Kommunikationspartner momentan online ist. Falls ein Kommunikationspartner offline ist, kann ihm keine Sofortnachricht übermittelt werden. Die Sofornachrichten-Übersichtsseite zeigt die letzten Streams an. Das System speichert eine begrenze Zahl von Sofortnachrichten. Es werden max. die letzten 100 Sofortnachrichten eines Benutzers angezeigt.

12 UC Suite

UC Suite bietet Unified Communications Leistungsmerkmale wie z. B. Anwesenheitsstatus und CallMe, Konferenzen sowie Sprach- und Faxnachrichten in den Clients myPortal for Desktop und myPortal for Outlook. myAttendant bietet zusätzlich Vermittlungsplatz-Funktionen.

INFO: UC Suite erfordert UC Server.

12.1 Grundeinstellungen für UC Suite

Grundlegende Einstellungen zu UC Suite können angepasst werden.

Die UC Suite kann aktiviert oder deaktiviert werden. Wenn UC Suite genutzt wird, muss UC Smart deaktiviert werden.

Zusätzlich können alle vom System eingeleiteten UC-Anrufe (z. B. über den CallMe-Dienst) vor der Wahl geprüft werden, ob der anfordernde UC Benutzer die Berechtigung für diesen Anruf hat. Fehlt dem UC Benutzer die Berechtigung, wird der Anruf nicht ausgeführt.

Verwandte Themen

- Wie Sie die IP-Adressen von Komponenten des Systems ermitteln

12.1.1 Wie Sie UC Suite aktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Applikationen > Applikationsauswahl**.

3) Klicken Sie im Menübaum auf **Applikations Auswahl > Applikations Auswahl**.

4) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie UC Suite mit UC Booster Card nutzen möchten, klicken Sie auf **Paket mit UC Suite**.
- Wenn UC Suite mit UC Booster Server nutzen möchten, klicken Sie auf **Paket mit UC Suite auf OSBiz UC Booster-Server** und geben Sie zusätzlich im Feld **IP-Adresse des OSBiz UC Booster-Servers** die IP-Adresse des externen Linux-Servers an.

5) Klicken Sie auf **Übernehmen**.

12.1.2 Wie Sie die Berechtigung von systemseitig eingeleiteten UC-Anrufe einschränken

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telephonie > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **Grundeinstellungen > System > System Flags**.

4) Wenn vor der Wahl von UC-Anrufen, die vom System eingeleitet werden, geprüft werden soll, ob der anfordernde UC Suite Benutzer die Berechtigung für diesen Anruf hat, aktivieren Sie im Bereich **Einschränkung für UC-Anrufe** das Kontrollkästchen **Einschränkung für UC-Anrufe**.

5) Wenn vor der Wahl von UC-Anrufen, die vom System eingeleitet werden, nicht geprüft werden soll, ob der anfordernde UC Suite Benutzer die Berechtigung für diesen Anruf hat, deaktivieren Sie im Bereich **Einschränkung für UC-Anrufe** das Kontrollkästchen **Einschränkung für UC-Anrufe**.

6) Klicken Sie auf **Übernehmen**.

12.2 UC Suite Clients

UC Suite Clients bieten Teilnehmern komfortable Oberflächen für umfangreiche Unified Communications-Funktionen.

Das System bietet folgende UC Suite Clients für folgende Geräte:

Client-Typ	Client	Gerät
Communications Client	myPortal for Desktop	PC
	myPortal for Outlook	
	Fax Printer	
	myAttendant	
	myPortal for OpenStage (UC Suite)	OpenStage Telefon

Client-Typ	Client	Gerät
Mobile Client	myPortal for Mobile (UC Suite) (siehe *Mobility*)	Mobiltelefon, Tablet-PC
	myPortal to go (UC Suite) (siehe *Mobility*)	Smartphone
Contact Center Client	myAgent (siehe *Multimedia Contact Center*)	PC
	myReports (siehe *Multimedia Contact Center*)	

Teilnehmer mit konfigurierter E-Mail-Adresse erhalten eine Begrüßungs-E-Mail mit einer Anleitung für erste Schritte.

Teilnehmer-individuelle Einstellungen

Die teilnehmer-individuellen Einstellungen für myPortal for Desktop werden in ini-Dateien auf dem PC gespeichert. Dabei wird für jeden Benutzer eine eigene ini-Datei angelegt. Die teilnehmer-individuellen Einstellungen für myPortal for Outlook, myAttendant und Fax Printer werden in der Registry des PC gespeichert. Dadurch können unterschiedliche Benutzer die Applikationen myPortal for Desktop, myPortal for Outlook, myAttendant und Fax Printer über einen PC nutzen (Desk Sharing). Dies ermöglicht den Einsatz in Windows Terminalserver- und in Citrix-Server-Umgebungen. Dadurch können unterschiedliche Benutzer mit ihren PCs die Applikationen ohne lokale Installation nutzen.

12.2.1 myPortal for Desktop

myPortal for Desktop ist ein Client für Unified Communications an Ihrem PC. Neben komfortablen Wahlhilfen über Verzeichnisse und Favoriten, Informationen über den Anwesenheitsstatus anderer Teilnehmer, hat der Teilnehmer z. B. auch Zugriff auf Sprach- und Faxnachrichten.

myPortal for Desktop bietet folgende Leistungsmerkmale:

- Verzeichnisse
- Favoritenliste
- Journal
- Desktop-Wahl
- PopUp-Fenster
- Anwesenheitsstatus
- CallMe-Dienst mit ONS (One Number Service)
- Statusbezogene Anrufumleitung
- Persönlicher AutoAttendant
- Konferenz-Management
- Aufzeichnen von Konferenzen

- Aufzeichnen von Anrufen
- Instant Messaging
- Sprach- und Faxnachrichten

12.2.1.1 Wie Sie eine alternative moderne Benutzeroberfläche für myPortal for Desktop bereitstellen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Führen Sie die folgenden Schritte durch, um eine alternative moderne Benutzeroberfläche für myPortal for Desktop mit benutzerdefiniertem Aussehen bereitzustellen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.
3) Klicken Sie auf **Bearbeiten** um den Wizard **Skin-Einstellungen** zu starten.
4) Klicken Sie auf **Durchsuchen** und wählen Sie die gewünschte Datei aus.
5) Klicken Sie auf **Upload**.
6) Wählen Sie eine der folgenden Möglichkeiten für die zu verwendende Schriftfarbe:
   - Wenn Sie weiße Schrift verwenden möchten, aktivieren Sie das Kontrollkästchen **Weiße Schrift verwenden**.
   - Wenn Sie weiße Schrift verwenden möchten, aktivieren Sie das Kontrollkästchen **Schwarze Schrift verwenden**.

12.2.1.2 Wie Sie die alternative moderne Benutzeroberfläche für myPortal for Desktop löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.
3) Klicken Sie auf **Bearbeiten** um den Wizard **Skin-Einstellungen** zu starten.
4) Klicken Sie auf **Löschen**.

12.2.2 myPortal for Outlook

myPortal for Outlook ist der Client für Unified Communications in Microsoft Outlook (Plug-In) analog zu myPortal for Desktop.

myPortal for Outlook bietet zusätzlich zu myPortal for Desktop folgende Leistungsmerkmale:

- Outlook-Kontakt anrufen
- Absender einer Sprachnachricht als Outlook-Kontakt anlegen
- Sprachnachricht als E-Mail senden
- Faxnachricht als E-Mail senden

12.2.3 Fax Printer

Fax Printer ist eine Windows-Anwendung für den Versand von Faxnachrichten aus anderen Windows-Anwendungen wie z. B. Microsoft Word mit individuell erstellten Deckblättern.

Fax Printer besteht aus folgenden Komponenten:

- Fax Printer Cover Editor
- Fax Printer Driver - mit folgenden Leistungsmerkmalen:
  - Faxversand an einzelne Empfänger
  - Verzeichnisse
  - Verwendung zentraler Deckblätter
  - Verwendung vordefinierter Kopfzeilen
  - Serienfax
  - Steuerung über die Benutzeroberfläche
  - Steuerung über die Kommandozeile

12.2.4 myAttendant

myAttendant ist eine Unified-Communications-Anwendung für Vermittlungsfunktionen. Neben komfortablen Vermittlungsfunktionen, Wahlhilfen über Verzeichnisse und Informationen über den Anwesenheitsstatus von Teilnehmern besteht z. B. auch Zugriff auf Sprach- und Faxnachrichten. Instant Messaging unterstützt die Kommunikation mit internen Teilnehmern.

myAttendant bietet folgende Leistungsmerkmale:

- Vermittlungsfunktionen
- Verzeichnisse
- Journal
- Pop-Up-Fenster
- Anwesenheitsstatus von Teilnehmern ändern

- Aufzeichnen von Anrufen
- Nachrichten-Center
- Teilnehmerschaltflächen
- Verwaltung von Sprach- und Faxnachrichten
- Instant Messaging
- Teamfunktionen
- Konferenz-Management

12.2.5 myPortal for OpenStage (UC Suite)

myPortal for OpenStage ist das Benutzerportal für den Zugriff auf Unified-Communications-Funktionen des Systems an Ihrem OpenStage-Telefon.

Die Konfiguration von myPortal for OpenStage ist über das OpenStage Telefon sowie über OpenStage Manager im Webbrowser möglich.

myPortal for OpenStage bietet folgende Leistungsmerkmale:

- Anwesenheitsstatus
- Sprachnachrichten

12.2.6 Voraussetzungen für UC Suite PC-Clients

Um UC Suite PC-Clients zu nutzen muss der Client-PC eine geeignete Hardware- und Softwareausstattung haben. Für die Installation und automatische Updates sind konfigurationsabhängig Administrationsrechte erforderlich. Der nutzbare Funktionsumfang ist abhängig von den verwendeten Lizenzen.

INFO: Beachten Sie bitte unbedingt die aktuellen Hinweise in der Datei `ReadMe first`, die sich im Ablageverzeichnis der Installationsdateien befindet.

Telefone

Die UC Suite PC-Clients können in Verbindung mit folgenden Telefonen genutzt werden:

- OpenStage HFA und SIP
- OpenScape Desk Phone IP 35G/55G HFA und SIP
- OpenScape Desk Phone IP 35G Eco SIP
- OpenStage T
- SIP-Telefone mit 3PCC-Unterstützung
- Analoge Telefone
- OpenScape Personal Edition HFA und SIP
- OpenScape Business Cordless
- OpenScape Cordless IP

- optiPoint WL2 professional SIP

Ältere Geräte (z. B. optiPoint 410/420/500) werden teilweise noch unterstützt. Getestete und freigegebene Geräte entnehmen Sie bitte den jeweiligen Freigabemitteilungen.

> ***INFO:*** Bei analogen Telefonen und DECT-Telefonen wird die Briefkastenlampe nicht unterstützt und die Anzeige von Informationen im Display nur eingeschränkt unterstützt.

Betriebssystem

Die UC Suite PC-Clients können in Verbindung mit folgenden Betriebssystemen verwendet werden:

- Apple Mac OS X v10.7.3 Lion
- Apple Mac OS X v10.8.x Mountain Lion
- Microsoft Windows 8
- Microsoft Windows 7
- Microsoft Windows Vista
- Microsoft Windows XP
- Office 365 (Lokale Installation: Office 2013)
- Microsoft Windows 2012, 2008 R2, 2008 und 2003 Server als Microsoft Terminal Server
- Microsoft Windows 2008 R2, 2008 und 2003 Server als Citrix XenApp 5.0 oder 6.0 Server

> ***INFO:*** Das verwendete Betriebssystem benötigt stets den aktuellen Stand aller verfügbaren Updates (Service Packs und Patches).

Der Support der UC Suite PC-Clients für Microsoft Office 2003, Microsoft Windows XP und Microsoft Windows 2003 Server endet zeitgleich mit der Betreuungseinstellung durch Microsoft. Das Produkt wird weiterhin unterstützt, jedoch nicht mehr detailliert getestet.

Die Installation unter Windows erfordert lokale Administrationsrechte auf einem Client-PC, automatische Updates jedoch nicht. Die russische bzw. chinesische Benutzeroberfläche von myPortal for Outlook erfordert eine russische bzw. chinesische Windows-Installation.

myPortal for Desktop für Apple MAC steht mit gleicher Oberfläche wie unter Microsoft Windows zur Verfügung. Aufgrund der Apple-MAC-OS-Systemarchitektur werden derzeit folgende Funktionen nicht unterstützt:

- Fax versenden
- Outlook, Entourage Integration

myPortal for Outlook wird in Microsoft Office 365 Umgebungen unterstützt. Microsoft Office 365 ist eine Cloud-Anwendung. Darin enthalten sind unter anderem ein Exchange-Server für die zentrale Verteilung von E-Mails, sowie

auch die klassischen Microsoft Office-Produkte. OpenScape Business unterstützt Microsoft Office 365.

Folgende Funktionen können unter Microsoft Office 365 genutzt werden:

- Exchange Kalender Integration
- E-Mail-Weiterleitung

Webbrowser

Für die Tastenprogrammierung der Telefone über die UC-Clients sind folgende Webbrowser freigegeben:

- Microsoft Internet Explorer Version 10 (oder neuer)
- Mozilla Firefox Version 19 (oder neuer)

Zusätzliche Software

zusätzliche Software	myPortal for Desktop	myAttendant	myPortal for Outlook
Oracle Java >= 1.6.031 oder 1.7.x (32 Bit oder 64 Bit)	X	X	
Microsoft Office 2013 (32 Bit oder 64 Bit) oder Microsoft Office 2010 (32 Bit oder 64 Bit) oder Microsoft Office 2007 (32 Bit oder 64 Bit) oder Microsoft Office 2003 (32 Bit) mit installierten .NET-Komponenten für Outlook oder Microsoft Office 365			X
Zugriff auf Microsoft Exchange-Server (für Outlook-Kontakte und -Termine) Exchange 2003 (32 Bit) Exchange 2013 (64 Bit) Exchange 2010 (64 Bit) Exchange 2007 (32 Bit)	X		X
Microsoft .NET Framework >= 3.5 (Outlook 2003/ 2007) oder Microsoft .NET Framework >= 4.0 (Outlook 2010/2013)			X

INFO: Für die Nutzung der Exchange-Kalender-Integration mit Microsoft Small Business Server muss in diesem unter Umständen FBA (Form Based Authentication) deaktiviert werden.

Hinweis zu Oracle Java 32 Bit oder 64 Bit

Bei Nutzung der myPortal for Desktop Funktion "Outlook-Kontakte beim Starten importieren" in Verbindung mit Microsoft Office 2013 in der 64 Bit Variante ist eine Installation von Oracle Java in der 64 Bit Variante erforderlich. Wird diese Funktion nicht verwendet, ist Oracle Java in der 32 Bit Variante zu empfehlen, da

somit der Arbeitsspeicher-Bedarf deutlich geringer ist. Bei allen anderen Installationen ist generell aus diesem Grund die 32 Bit Variante von Oracle Java empfohlen.

Hardware Mindestanforderungen

- 2 GHz CPU
- RAM: 2 GB
  (Microsoft Windows XP: 1 GB)
  (Microsoft Windows 2003 Server: 1 GB)
- 100 Mbit/s LAN (1 Gbit/s LAN empfohlen)
- XGA (1024x768) Bildschirmauflösung, myPortal for Outlook: SVGA (800x600) Bildschirmauflösung

Microsoft Terminalserver, Citrix XenApp Server

Die UC Suite PC-Clients können unter den nachfolgend genannten Voraussetzungen in Microsoft Terminalserver- und Citrix-Server-Umgebungen eingesetzt werden.

INFO: Terminalserver- und Citrix-Server-Umgebungen inklusive Hosted Services und virtuelle Umgebungen liegen in der Verantwortung des Kunden.

INFO: Citrix-Server-Umgebungen können einige regionale Buchstaben (z.B. deutsche Umlaute) nicht korrekt decodieren.

Betriebssystem:

- Microsoft Windows 2012 Server als Microsoft Terminal Server
- Microsoft Windows 2008 R2 Server als Microsoft Terminal Server
- Microsoft Windows 2008 Server als Microsoft Terminal Server
- Microsoft Windows 2003 Server als Microsoft Terminal Server
- Microsoft Windows 2008 R2 Server (64 Bit) mit Citrix XenApp 6.0 und 6.5 Server (Desktop Mode)
- Microsoft Windows 2008 R2 Server (64 Bit) mit Citrix XenApp 5.0 Server (Desktop Mode)

Office-Anwendungen:

- Microsoft Office 2013 (32 Bit und 64 Bit)
- Microsoft Office 2010 (32 Bit und 64 Bit)
- Microsoft Office 2007 (32 Bit)
- Microsoft Office 2003 (32 Bit)

Hardware-Voraussetzungen: Die Anzahl der installierbaren Clients hängt ab von der Server-Performance und dem zur Verfügung stehenden Arbeitsspeicher. Werden auf dem Server weitere Applikationen genutzt, ist deren Arbeitsspeicherbedarf zu berücksichtigen.

Weitere Informationen über die Konfiguration unter Citrix XenApp Server finden Sie unter:

`http://wiki.unify.com/wiki/OpenScape_Business`.

Installationsdateien

Für die Bereitstellung der Installationsdateien an die Benutzer bestehen folgende Möglichkeiten:

- Der Administrator lädt die Installationsdateien aus dem **Service-Center** herunter und stellt diese den Benutzern bereit, z. B. über ein Netzlaufwerk.

12.2.7 Voraussetzungen für myPortal for OpenStage (UC Suite)

Um myPortal for OpenStage zu nutzen muss das Telefon über geeignete Hardware und Software verfügen.

Telefone

myPortal for OpenStage kann mit folgenden Telefonen genutzt werden:

- OpenStage 60 ab V2
- OpenStage 80 ab V2

Webbrowser

myPortal for OpenStage kann in Verbindung mit folgenden Webbrowsern verwendet werden (für Konfiguration und Administration):

- Microsoft Internet Explorer Version 10 (oder neuer)
- Mozilla Firefox Version 19 (oder neuer)

12.2.8 Silent Installation/Deinstallation für UC Suite PC-Clients

Silent Installation/Deinstallation ist eine kommandozeilenbasierte Methode zur automatischen Installation, Deinstallation und Modifikation von UC Suite PC-Clients auf einem PC ohne weitere erforderliche Eingaben.

> ***INFO:*** Beachten Sie bitte unbedingt die Hinweise in der Datei `ReadMe first.rtf`.

Silent Installation/Deinstallation ist ab V3 verfügbar und erfordert lokale Administrationsrechte auf dem betreffenden PC. Silent Installation/Deinstallation ermöglicht die Protokollierung des Ablaufs in einer Datei.

Für Silent Installation/Deinstallation stehen folgende Parameter zur Verfügung:

Parameter	Komponenten
`ALL`	• myPortal for Desktop / myAttendant • myPortal for Outlook • Fax Printer • myAgent • Automatische Updates
`myPortal`	myPortal for Desktop / myAttendant
`OutlookIntegration`	myPortal for Outlook
`FaxPrinter`	Fax Printer
`myAgent`	myAgent

12.2.8.1 Wie Sie eine Silent Installation durchführen

Voraussetzungen

- Ihr PC erfüllt die *Voraussetzungen für UC Suite PC-Clients*.
- Sie verfügen über lokale Administrationsrechte auf dem Client-PC.
- Die Datei `CommunicationsClients.exe` ist am Client-PC verfügbar.

> ***INFO:*** Beachten Sie bitte unbedingt die Hinweise in der Datei `ReadMe first`.

Benutzen Sie Kommandozeilen nach den folgenden Mustern in einer Batch-Datei oder in einem Fenster mit der DOS-Eingabeaufforderung.

Schritt für Schritt

1) Wenn Sie den Ablauf nicht protokollieren möchten, wählen Sie eine der folgenden Kommandozeilen:

> ***INFO:*** Beachten Sie bei Parametern die exakte Schreibweise in Groß- und Kleinbuchstaben.

- Wenn Sie alle Komponenten installieren möchten:
  `CommunicationsClients.exe /passive ADDLOCAL=ALL`
- Wenn Sie mehrere Komponenten installieren möchten, geben Sie deren entsprechende Parameter als Aufzählung getrennt durch Komma an nach `ADDLOCAL=`, z. B. myPortal for Desktop / myAttendant und Fax Printer:
  `CommunicationsClients.exe /passive ADDLOCAL=myPortal,FaxPrinter`

- Wenn Sie nur eine Komponente installieren möchten, geben Sie den entsprechenden Parameter an nach `ADDLOCAL=`, z. B. myPortal for Desktop / myAttendant:

  ```
  CommunicationsClients.exe /passive ADDLOCAL=myPortal
  ```

2) Wenn Sie den Ablauf in einer Datei, z. B. `C:\ccinstall.log`, protokollieren möchten, wählen Sie eine der folgenden Kommandozeilen:

> ***INFO:*** Beachten Sie bei Parametern die exakte Schreibweise in Groß- und Kleinbuchstaben.

- Wenn Sie alle Komponenten installieren möchten:

  ```
  CommunicationsClients.exe /passive /L*V
  "C:\ccinstall.log" ADDLOCAL=ALL
  ```

- Wenn Sie mehrere Komponenten installieren möchten, geben Sie deren entsprechende Parameter als Aufzählung getrennt durch Komma an nach `ADDLOCAL=`, z. B. myPortal for Desktop / myAttendant und Fax Printer:

  ```
  CommunicationsClients.exe /passive /L*V
  "C:\ccinstall.log" ADDLOCAL=myPortal,FaxPrinter
  ```

- Wenn Sie nur eine Komponente installieren möchten, geben Sie den entsprechenden Parameter an nach `ADDLOCAL=`, z. B. myPortal for Desktop / myAttendant:

  ```
  CommunicationsClients.exe /passive /L*V
  "C:\ccinstall.log" ADDLOCAL=myPortal
  ```

12.2.8.2 Wie Sie eine Silent Deinstallation durchführen

Voraussetzungen

- Ihr PC erfüllt die *Voraussetzungen für UC Suite PC-Clients*.
- Sie verfügen über lokale Administrationsrechte auf dem Client-PC.
- Die Datei `CommunicationsClients.exe` ist am Client-PC verfügbar.

> ***INFO:*** Beachten Sie bitte unbedingt die Hinweise in der Datei `ReadMe first`.

Benutzen Sie Kommandozeilen nach den folgenden Mustern in einer Batch-Datei oder in einem Fenster mit im Fenster mit der DOS-Eingabeaufforderung.

Schritt für Schritt

1) Wenn nach der letzten Silent Installation ein Update des Systems durchgeführt wurde, wiederholen Sie mit der neuen Datei `CommunicationsClients.exe` genau jene Kommandozeilen, die Sie mit der bisherigen Datei `CommunicationsClients.exe` durchgeführt haben (so, als ob Sie die

bereits installierten Komponenten mit der neuen Datei `CommunicationsClients.exe` neu installieren wollten). Erst anschließend ist Silent Deinstallation möglich.

2) Wenn Sie den Ablauf nicht protokollieren möchten, wählen Sie eine der folgenden Kommandozeilen:

> ***INFO:*** Beachten Sie bei Parametern die exakte Schreibweise in Groß- und Kleinbuchstaben.

- Wenn Sie alle Komponenten deinstallieren möchten:

  ```
  CommunicationsClients.exe /passive REMOVE=ALL
  ```

- Wenn Sie mehrere Komponenten deinstallieren möchten, geben Sie deren entsprechende Parameter als Aufzählung getrennt durch Komma an nach `REMOVE=`, z. B. myPortal for Desktop / myAttendant und Fax Printer:

  ```
  CommunicationsClients.exe /passive
  REMOVE=myPortal,FaxPrinter
  ```

- Wenn Sie nur eine Komponente deinstallieren möchten, geben Sie den entsprechenden Parameter an nach `REMOVE=`, z. B. myPortal for Desktop / myAttendant:

  ```
  CommunicationsClients.exe /passive REMOVE=myPortal
  ```

3) Wenn Sie den Ablauf z. B. in einer Datei, z. B. `C:\ccuninstall.log`, protokollieren möchten, wählen Sie eine der folgenden Kommandozeilen:

> ***INFO:*** Beachten Sie bei Parametern die exakte Schreibweise in Groß- und Kleinbuchstaben.

- Wenn Sie alle Komponenten deinstallieren möchten:

  ```
  CommunicationsClients.exe /passive /L*V "C:\ccuninstall.log" REMOVE=ALL
  ```

- Wenn Sie mehrere Komponenten deinstallieren möchten, geben Sie deren entsprechende Parameter als Aufzählung getrennt durch Komma an nach `REMOVE=`, z. B. myPortal for Desktop / myAttendant und Fax Printer:

  ```
  CommunicationsClients.exe /passive /L*V "C:\ccuninstall.log" REMOVE=myPortal,FaxPrinter
  ```

- Wenn Sie nur eine Komponente deinstallieren möchten, geben Sie den entsprechenden Parameter an nach `REMOVE=`, z. B. myPortal for Desktop / myAttendant:

  ```
  CommunicationsClients.exe /passive /L*V "C:\ccuninstall.log" REMOVE=myPortal
  ```

12.2.9 Automatische Updates

Automatische Updates halten UC Clients auf dem neuesten Stand.

Ist eine neue Version verfügbar, wird diese entweder automatisch aktualisiert oder es wird über die Möglichkeit der Aktualisierung informiert. Gegebenenfalls erscheint eine Meldung, dass eine oder mehrere Anwendungen beenden werden müssen um das Update durchzuführen.

INFO: Es wird empfohlen, die angebotenen Updates stets durchzuführen. Dies gilt ebenso für Software, die für bestimmte UC Clients erforderlich ist.

12.3 Benutzer und Benutzer-Profile von UC Suite

Benutzer von UC Suite sind Teilnehmer, welche UC Clients von UC Suite nutzen. Benutzer-Profile speichern Einstellungen von Benutzern von UC Suite.

12.3.1 Benutzer von UC Suite

Benutzer von UC Suite nutzen UC Clients von UC Suite. Die Einstellungen der Benutzer von UC Suite sind im Benutzerverzeichnis konfigurierbar.

Das Benutzerverzeichnis enthält alle Teilnehmer des Systems. Für die Benutzung der UC Clients sind zusätzliche Benutzerdaten im Benutzerverzeichnis zu konfigurieren.

Im Benutzerverzeichnis werden zu jedem Benutzer folgende Informationen angezeigt:

- Symbol für Anwesenheitsstatus
  Der Administrator kann den Anwesenheitsstatus für jeden Benutzer ändern.
- **Nebenstelle**
- **Benutzername**
  Frei definierbar.
- **Name**
  Vor- und Nachname, wie für den Teilnehmer konfiguriert.
- **Abteilung**
  Falls dem Benutzer eine Abteilung zugeordnet ist.
- **E-Mail**
  E-Mail-Adresse
- **Ist Agent**
  Agentenlevel im Multimedia Contact Center.

- **Sprachnachrichten**
  Der Benutzer kann Sprachnachrichten empfangen.
- **Umleitung**
  Für den Benutzer ist eine Anrufumleitung konfiguriert.

Folgende Einstellungen können konfiguriert werden:

Werte und Einstellungen	Stichworte
Persönliche Daten	
Eigene persönliche Daten	Eigenen Namen, Benutzername, Kennwort, E-Mail-Adresse, Abteilung, Zusätzliche Rufnummer, XMPP-ID
Eigenes Bild	Eigenes Bild
Benutzerebene	Empfang von Sprachnachrichten: siehe *Teilnehmer* Benutzer als Vermittlungsplatz: siehe *Teilnehmer* Benutzer als Agent: siehe *Teilnehmer*
Meine Einstellungen	
Darstellung	Skin-Farben, Sprache der Benutzeroberfäche
Benachrichtigungen	PopUp-Fenster
Kalender-Anbindung	Automatische Erstellung von Outlook-Terminen bei Abwesenheit, Automatische Aktualisierung des Anwesenheitsstatus durch Outlook-/iCal-Termine
Abkürzungstasten	Abkürzungstaste für Funktionen
Verschiedenes	Automatisches Zurücksetzen des Anwesenheitsstatus, Übergabemethode, Aufbewahrungsdauer für Journaleinträge, Serveradresse, Funktionstasten des Telefons
Anrufregeln	
Anrufweiterleitungsziele	Statusbezogene Anrufumleitung
Regelmodul	Regelbasierte Anrufumleitung
Kommunikation	
Einstellungen für Sprachnachrichten	Aufzeichnungs- oder Ansagemodus, Sprache der Sprachbox
Sprachnachricht-Benachrichtigung	Benachrichtigungsdienst für neue Nachrichten
Fax-Benachrichtigung	Benachrichtigungsdienst für neue Nachrichten
Profile	
Besetzt, Nicht angenommen, Besprechung, Krank, Pause, Außer Haus, Urlaub, Mittagspause, Privat	Profil für persönlichen AutoAttendant
Sensibilität	
Sicherheit und Zugriff	Abrufen Ihrer Sprach- und Faxnachrichten durch die Vermittlung, Kennwortabfrage der Sprachbox

Werte und Einstellungen	Stichworte
Sichtbarkeit des Anwesenheits-status	Sichtbarkeit Ihres Anwesenheitsstatus für Andere
VoiceMail-Anwesenheitsstatus	Ansage Ihres Anwesenheitsstatus für externe Anrufer, Ansage Ihres Anwesenheitsstatus für bestimmte Anru-fer
myAttendant	
LAN-Nachrichten	Textbaustein für Sofortnachrichten
DuWas	Durchwahlnummer
Kommunikation	Anrufweiterleitungen

Weitere Informationen zu den Einstellungen der Benutzer finden Sie in den Bedienungsanleitungen der UC Clients unter den in der Tabelle aufgeführten Stichworten.

Das Kennworts für UC Clients ist standardmäßig sechsstellig. Die Länge des Kennworts kann an den eigenen Bedarf angepasst werden (6-10 Stellen). Ein Administrator mit dem Profil **Advanced** kann das Kennwort eines Benutzers ändern (z. B. falls es der Benutzer vergessen hat).

INFO: Vor- und Nachname eines Benutzers werden im Benutzer-verzeichnis überschrieben, wenn sie über einen Wizard oder über den Experten-Modus geändert werden. Werden dagegen Vor- und Nachname eines Benutzers im Benutzerverzeichnis geändert, werden die Daten des Benutzers, wie sie über einen Wizard oder über den Experten-Modus angezeigt werden, nicht überschrieben. In diesem Fall existieren zwei unterschiedliche Benutzernamen für denselben Benutzer.

Teilnehmer, für die eine E-Mail-Adresse konfiguriert ist und die myPortal for Desktop nutzen, erhalten eine Begrüßungs-E-Mail mit einer Erste-Schritte-Anleitung.

Benutzerdaten zurücksetzen

DieEinstellungen eines Benutzers können auf Standardwerte zurückgesetzt werden. Dabei werden auch seine Sprachnachrichten, persönliche Ansagen der Sprachbox, Journaleinträge, geplante Konferenzen, E-Mails und Faxnachrichten gelöscht.

12.3.1.1 Wie Sie einen Benutzer von UC Suite konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Benutzerverzeichnis** zu starten. Es werden alle Benutzer angezeigt.
4) Markieren Sie den gewünschten Benutzer und klicken Sie auf **Bearbeiten**.
5) Ändern Sie die Daten des Benutzers.
6) Klicken Sie auf **Speichern**. Das Fenster wird automatisch geschlossen. Es werden alle Benutzer angezeigt.
7) Wenn Sie einen weiteren Benutzer konfigurieren möchten, wiederholen Sie die Schritte 4 bis 6.

12.3.1.2 Wie Sie einen Benutzer von UC Suite zurücksetzen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Benutzerverzeichnis** zu starten. Es werden alle Benutzer angezeigt.
4) Markieren Sie den gewünschten Benutzer und klicken Sie auf **Benutzer zurücksetzen**.
5) Klicken Sie auf **Speichern**. Das Fenster wird automatisch geschlossen. Es werden alle Benutzer angezeigt.
6) Wenn Sie einen weiteren Benutzer zurücksetzen möchten, wiederholen Sie die Schritte 4 bis 5.

12.3.1.3 Wie Sie einen Benutzer von UC Suite als Agenten konfigurieren (myAgent)

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Benutzerverzeichnis** zu starten. Es werden alle Benutzer angezeigt.

4) Klicken Sie in die Zeile mit dem entsprechenden Benutzer.

5) Klicken Sie auf **Bearbeiten**.

6) Klicken Sie auf **Persönliche Daten > Benutzerebene**.

7) Wählen Sie eine der folgenden Möglichkeiten:

   Wenn der Agent dauerverfügbar sein soll, aktivieren Sie das Kontrollkästchen **Dauerverfügbarer Agent**. Der Agent bleibt auch dann für Anrufe, Faxe und E-Mails verfügbar, wenn er einen Anruf, ein Fax oder eine E-Mail nicht angenommen hat.

   Wenn der Agent nicht dauerverfügbar sein soll, deaktivieren Sie das Kontrollkästchen **Dauerverfügbarer Agent**. Der Agent erhält den Zustand nicht verfügbar, wenn er einen Anruf, ein Fax oder eine E-Mail nicht angenommen hat.

8) Wählen Sie in der Aufklappliste **Level** die für diesen Agenten gewünschte Rolle: **Agent**, **Supervisor** oder **Adminsitrator**.

9) Klicken Sie auf **Speichern**.

10) Wenn Sie einen weiteren Benutzer als Agent konfigurieren möchten, wiederholen Sie die Schritte 4 bis 9.

12.3.1.4 Wie Sie für einen Benutzer von UC Suite den Anwesenheitsstatus ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Benutzerverzeichnis** zu starten. Es werden alle Benutzer angezeigt.

4) Markieren Sie den gewünschten Benutzer.

5) Wählen Sie in der Aufklappliste den betreffenden Anwesenheitsstatus aus und geben Sie gegebenenfalls den geplanten Zeitpunkt der Rückkehr im Format `jjjj/mm/tt hh:mm` ein, z. B. `2012/12/12 12:00`.

6) Klicken Sie auf **OK**.

7) Wenn Sie für einen weiteren Benutzer den Anwesenheitsstatus ändern möchten, wiederholen Sie die Schritte 4 bis 6.

8) Schließen Sie das Fenster.

12.3.1.5 Wie Sie für einen Benutzer von UC Suite das Kennwort ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Benutzerverzeichnis** zu starten. Es werden alle Benutzer angezeigt.
4) Markieren Sie den betreffenden Benutzer und klicken Sie auf **Bearbeiten**.
5) Klicken Sie unter **Kennwort** auf **Ändern**.
6) Geben Sie in **Neu** das neue Kennwort ein.
7) Geben Sie in **Bestätigen** das neue Kennwort ein.
8) Klicken Sie auf **OK**. Das Fenster wird automatisch geschlossen. Es werden alle Benutzer angezeigt.
9) Wenn Sie das Kennwort eines weiteren Benutzers ändern möchten, wiederholen Sie die Schritte 4 bis 8.

Nächste Schritte

Informieren Sie den bzw. die betroffenen Benutzer über das neue Kennwort.

12.3.1.6 Wie Sie für einen Benutzer von UC Suite die Kennwortlänge ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen > OpenScape Business UC Suite**.
3) Klicken Sie auf **Server**.
4) Klicken Sie auf **Allgemeine Einstellungen**.
5) Geben Sie in **Kennwortlänge** die künftig mindestens erforderliche Kennwortlänge (6-10) ein.
6) Klicken Sie auf **Speichern**.

12.3.2 Benutzer-Profile von UC Suite

Benutzer-Profilen von UC Suite speichern Einstellungen von Benutzern von UC Suite. Einem Benutzer-Profil können mehrere Benutzer (Mitglieder) zugeordnet werden. Alle Mitglieder dieses Profils haben die gleichen Einstellungen.

Jeder Benutzer kann Mitglied von höchstens einem Benutzer-Profil sein. Direkte Änderungen an den Einstellungen eines Benutzers - also nicht über das zugeordnetes Profil - löschen den Benutzer automatisch aus dem Profil.

Folgende Werte und Einstellungen können konfiguriert werden:

Menüpunkte	Werte und Einstellungen zu
Persönliche Daten	
Eigene persönliche Daten	Sichtbarkeit von Rufnummern
Meine Einstellungen	
Darstellung	Skin-Farben, Sprache der Benutzeroberfäche
Benachrichtigungen	PopUp-Fenster
Outlook-Anbindung	Automatische Erstellung von Outlook-Terminen bei Abwesenheit, Automatische Aktualisierung des Anwesenheitsstatus durch Outlook-/iCal-Termine
Verschiedenes	Automatisches Zurücksetzen des Anwesenheitsstatus, Übergabemethode, Aufbewahrungsdauer für Journaleinträge, Serveradresse
Anrufregeln	
Anrufweiterleitungsziele	Statusbezogene Anrufumleitung
Kommunikation	
Einstellungen für Sprachnachrichten	Aufzeichnungs- oder Ansagemodus, Sprache der Sprachbox
Sprachnachricht-Benachrichtigung	Benachrichtigungsdienst für neue Nachrichten
Fax-Benachrichtigung	Benachrichtigungsdienst für neue Nachrichten
Profile	
Besetzt, Nicht angenommen, Besprechung, Krank, Pause, Außer Haus, Urlaub, Mittagspause, Privat	Profil für persönlichen AutoAttendant
Sensibilität	

Menüpunkte	Werte und Einstellungen zu
Sicherheit und Zugriff	Abrufen Ihrer Sprach- und Faxnachrichten durch die Vermittlung, Kennwortabfrage der Sprachbox
Sichtbarkeit des Anwesenheitsstatus	Sichtbarkeit Ihres Anwesenheitsstatus für Andere
VoiceMail-Anwesenheitsstatus	Ansage Ihres Anwesenheitsstatus für externe Anrufer, Ansage Ihres Anwesenheitsstatus für bestimmte Anrufer

Weitere Informationen zu Einstellungen der Benutzer-Profile finden Sie in den Bedienungsanleitungen der UC Clients unter den in der Tabelle aufgeführten Stichworten.

12.3.2.1 Wie Sie ein Benutzer-Profil von UC Suite hinzufügen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Profile** zu starten. Es werden alle Benutzer-Profile und deren Mitglieder angezeigt.

4) Klicken Sie auf **Hinzufügen**.

5) Geben Sie in **Name** den gewünschten Namen für das Profil ein.

6) Klicken Sie auf **Speichern**.

7) Konfigurieren Sie die gewünschten Einstellungen des Benutzer-Profils.

8) Klicken Sie auf **Speichern** und schließen Sie das Fenster.

12.3.2.2 Wie Sie ein Benutzer-Profil von UC Suite ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Profile** zu starten. Es werden alle Profile und deren Benutzer angezeigt.

4) Markieren Sie das gewünschte Profil.

5) Klicken Sie auf **Bearbeiten**.

6) Ändern Sie die gewünschten Werte und Einstellungen.

> ***INFO:*** Klicken Sie auf **Speichern** bevor Sie zu einem anderen Menüpunkt wechseln, damit Ihre Änderungen übernommen werden.

7) Klicken Sie abschließend auf **Speichern** und schließen Sie das Fenster.

12.3.2.3 Wie Sie die Benutzer-Profile von UC Suite anzeigen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Profile** zu starten. Es werden alle Benutzer-Profile und deren Mitglieder angezeigt.

12.3.2.4 Wie Sie Mitglieder zu einem Benutzer-Profil von UC Suite hinzufügen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Profile** zu starten. Es werden alle Benutzer-Profile und deren Mitglieder angezeigt.

4) Markieren Sie das gewünschte Benutzer-Profil und klicken Sie auf **Benutzer zuordnen**.

5) Wählen Sie aus der Liste **Verfügbare Benutzer** die gewünschten Mitglieder aus.

6) Klicken Sie auf **<-** um diese in die in die Liste **Zugewiesene Benutzer** zu übernehmen.

Es werden alle Teilnehmer-Profile und deren Mitglieder angezeigt.

7) Schließen Sie das Fenster.

12.3.2.5 Wie Sie Mitglieder aus einem Benutzer-Profil von UC Suite löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Profile** zu starten. Es werden alle Benutzer-Profile und deren Mitglieder angezeigt.
4) Markieren Sie das gewünschte Benutzer-Profil und klicken Sie auf **Benutzer zuordnen**.
5) Wählen Sie aus der Liste **Zugewiesene Benutzer** die betreffenden Mitglieder aus.
6) Klicken Sie diese auf **->** um diese in die Liste **Verfügbare Benutzer** zu übernehmen.

   Es werden alle Teilnehmer-Profile und deren Mitglieder angezeigt.
7) Schließen Sie das Fenster.

12.3.2.6 Wie Sie ein Benutzer-Profil von UC Suite löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Profile** zu starten. Es werden alle Benutzer-Profile und deren Mitglieder angezeigt.
4) Markieren Sie das gewünschte Benutzer-Profil.
5) Klicken Sie auf **Entfernen**.
6) Bestätigen Sie mit **OK**. Es werden alle Teilnehmer-Profile und deren Mitglieder angezeigt.
7) Schließen Sie das Fenster.

12.4 Anwesenheitsstatus und CallMe-Dienst

Anwesenheitsstatus und CallMe-Dienst zeigen und optimieren die Erreichbarkeit von Teilnehmern. Der Anwesenheitsstatus ermöglicht eine einfache statusbe-

zogene Anrufumleitung sowie eine mit myPortal for Desktop bzw. myPortal for Outlook flexibel konfigurierbare regelbasierte Anrufumleitung.

12.4.1 Anwesenheitsstatus (UC Suite)

Der Anwesenheitsstatus (Präsenz, Presence) informiert in der Favoritenliste, im internen Verzeichnis, im virtuellen Konferenzraum und durch Ansagen der Sprachbox über die Verfügbarkeit interner Teilnehmer (auch mobile Teilnehmer). Darüber hinaus steuert der Anwesenheitsstatus die Erreichbarkeit interner Teilnehmer mit der statusbezogenen Anrufumleitung, der regelbasierten Anrufumleitung und dem persönlichen AutoAttendant.

Sie können als Teilnehmer Ihren Anwesenheitsstatus in myPortal for Desktop, myPortal for Outlook oder über die Menüsteuerung der Sprachbox ändern. Durch Deaktivieren einer Anrufumleitung am Telefon kehren Sie zum Anwesenheitsstatus **Büro** zurück. Bei jeder Änderung des Anwesenheitsstatus außer für **Büro** und **CallMe** legen Sie den Zeitpunkt der geplanten Rückkehr zu **Büro** bzw. **CallMe** fest.

Als Teilnehmer können Sie folgende Status auswählen:

- **Büro**
- **Besprechung**
- **Krank**
- **Pause**
- **Außer Haus**
- **Urlaub**
- **Mittagspause**
- **Zu Hause**
- **Anrufschutz**
  (nicht verfügbar bei Mobility Entry oder MULAP)

Mapping des XMPP-Status von extern

Teilnehmer können den Anwesenheitsstatus externer XMPP-Kommunikationspartner sehen, z. B. in der Favoritenliste oder im externen Verzeichnis, sofern XMPP konfiguriert ist. Dabei gilt folgende Zuordnung (von links nach rechts):

XMPP-Status	dargestellt als Anwesenheitsstatus
Online	Büro
DND	Besprechung
Away	Außer Haus
Extended Away	Urlaub

INFO: Outlook-Kontakte müssen die XMPP-ID im Feld IM-Adresse nach folgendem Muster enthalten:
`xmpp:john.public@oso.example-for-a-domain`.

Mapping des Anwesenheitsstatus nach extern

Externe XMPP-Kommunikationspartner können den XMPP-Status von Teilnehmern sehen, sofern XMPP konfiguriert ist. Dabei gilt folgende Zuordnung (von links nach rechts):

Anwesenheitsstatus	dargestellt als XMPP-Status
Büro	Online
Besprechung	DND
Krank	Away
Pause	Away
Außer Haus	Away
Mittagspause	Away
Zu Hause	Away
Urlaub	Extended Away

Umleitung zur Sprachbox

Wenn der Anwesenheitsstatus eines Teilnehmers nicht **Büro** oder **CallMe** ist, leitet das Kommunikationssystem Anrufe für ihn standardmäßig zur Sprachbox um und informiert durch statusbezogene Ansagen über die Art seiner Abwesenheit und den geplanten Zeitpunkt seiner Rückkehr.

Informationstext

Sie können zu Ihrem aktuellen Anwesenheitsstatus einen beliebigen Informationstext eingeben, z. B. bei einer Besprechung: "Bin in Raum Nr. ...". Der Informationstext wird in der Favoritenliste, im internen Verzeichnis und im virtuellen Konferenzraum angezeigt. Der Informationstext wird bei Änderung Ihres Anwesenheitsstatus gelöscht.

Automatisches Zurücksetzen des Anwesenheitsstatus

Sie können als Teilnehmer zum geplanten Ende-Zeitpunkt Ihrer Abwesenheit den Anwesenheitsstatus automatisch auf **Büro** zurücksetzen lassen. Anderenfalls verlängert das System den aktuellen Anwesenheitsstatus in 15-Minuten-Schritten bis Sie ihn selbst ändern.

Sichtbarkeit Ihres Anwesenheitsstatus

Sie können als Teilnehmer für jeden Teilnehmer des internen Verzeichnisses festlegen, ob dieser Ihren Anwesenheitsstatus abweichend von **Büro** und **CallMe** sowie den geplanten Zeitpunkt Ihrer Rückkehr und von Ihnen eventuell eingegebenen Informationstext sehen kann.

Automatische Aktualisierung des Anwesenheitsstatus durch Outlook-/iCal-Termine

Sie können als Teilnehmer Ihren Anwesenheitsstatus durch Termine (nicht jedoch abgesagte oder lediglich vorgeschlagene) mit bestimmten Schlüsselwörtern im Betreff automatisch steuern. Sie können zwischen folgenden Kalendern wählen:

- Exchange-Kalender (auf dem Microsoft Exchange Server)
  Die automatische Aktualisierung des Anwesenheitsstatus durch Outlook-Termine erfolgt unabhängig davon, ob Ihr PC in Betrieb ist. Für diese Funktion muss der Administrator die Exchange-Kalender-Integration konfigurieren.

  INFO: Details zur Nutzung der verschiedenen Microsoft Exchange Server Versionen finden Sie im Unify Experts Wiki unter: `http://wiki.unify.com/wiki/OpenScape_Business#Microsoft_Exchange_Server`.

- Outlook-Kalender
  Die automatische Aktualisierung des Anwesenheitsstatus durch Outlook-Termine erfordert, dass myPortal for Desktop oder myPortal for Outlook auf Ihrem PC gestartet ist.
- iCal-Kalender (myPortal for Desktop)

Sie können die folgenden Schlüsselwörter verwenden:

- **Besprechung**
- **Krank**
- **Pause**
- **Außer Haus**
- **Urlaub**
- **Mittagspause**
- **Zu Hause**

Die Schlüsselwörter hängen von der eingestellten Sprache der Benutzeroberfläche ab. Die Schlüsselwörter dürfen im Betreff an beliebiger Stelle stehen. Wenn der Betreff mehrere dieser Schlüsselwörter enthält, wird nur das erste wirksam. Wenn diese Funktion aktiviert ist, ändert sich Ihr Anwesenheitsstatus zur Beginn- und Endezeit des betreffenden Termins automatisch. Die Prüfung des Kalenders auf Termine erfolgt in Intervallen von 30 s.

HINWEIS: Wenn Sie diese Funktion aktivieren, beachten Sie bitte, dass beliebige Termine mit entsprechenden Schlüsselwörtern im Betreff zu unerwünschten Änderungen Ihres Anwesenheitsstatus führen können. Ändern Sie gegebenenfalls den Betreff.

Automatische Erstellung von Outlook-Terminen bei Abwesenheit (Windows)

Sie können als Teilnehmer für Ihre Abwesenheit automatisch entsprechende Outlook-Termine durch Änderung Ihres Anwesenheitsstatus erzeugen lassen.

Der Betreff des entsprechenden Outlook-Termins besteht aus Ihrem Anwesenheitsstatus und dem Text "(Auto)", z. B. "Besprechung (Auto)". Beginn- und Endezeit des betreffenden Termins entsprechen Ihren Angaben in myPortal for Desktop oder myPortal for Outlook. Die Endezeit des Outlook-Termins bleibt bei einer eventuell verspäteten Rückkehr unverändert. Sie können festlegen, ob die Outlook-Termine in der lokalen PST-Datei oder auf dem Exchange-Server gespeichert werden. Im Fall der lokalen PST-Datei muss Ihr Outlook zum Erstellen der Outlook-Termine geöffnet sein. Im Fall des Exchange-Servers werden die Outlook-Termine erstellt, unabhängig davon, ob Ihr Outlook geöffnet ist. Für diese Funktion muss der Administrator die Exchange-Kalender-Integration konfigurieren.

INFO: Details zur Nutzung der verschiedenen Microsoft Exchange Server Versionen finden Sie im Unify Experts Wiki unter `http://wiki.unify.com/wiki/OpenScape_Business#Microsoft_Exchange_Server`.

PopUp-Fenster bei Änderung des Anwesenheitsstatus

Sie können als Teilnehmer Änderungen Ihres Anwesenheitsstatus durch PopUp-Fenster anzeigen lassen.

12.4.2 CallMe-Dienst

Mit dem CallMe-Dienst kann ein Teilnehmer ein beliebiges Telefon an einem alternativen Arbeitsplatz als CallMe-Ziel festlegen, an dem er unter seiner internen Telefonnummer erreichbar ist. Der Teilnehmer kann myPortal for Desktop oder myPortal for Outlook an seinem alternativen Arbeitsplatz wie im Büro nutzen und damit auch gehende Anrufe vom CallMe-Ziel tätigen.

Ankommende Anrufe

Ankommende Anrufe bei der internen Telefonnummer werden zum CallMe-Ziel umgeleitet. Beim Anrufer wird die interne Telefonnummer des gerufenen Teilnehmers angezeigt. Nicht angenommene Anrufe werden nach 60 Sekunden an die Sprachbox weitergeleitet.

Gehende Anrufe

Bei gehenden Anrufen mit myPortal for Desktop oder myPortal for Outlook baut das Kommunikationssystem zwei Verbindungen auf. Zuerst ruft das Kommunikationssystem den Teilnehmer am CallMe-Ziel an. Wenn er den Anruf annimmt, ruft das Kommunikationssystem das gewünschte Ziel und verbindet ihn mit diesem. Am Ziel wird die interne Telefonnummer des Anrufenden angezeigt (One Number Service).

Anwesenheitsstatus

Bei aktiviertem CallMe-Dienst erscheint im Display des betreffenden Telefons "`CallMe aktiv`" (nicht für analoge Telefone und DECT-Telefone). Andere Teilnehmer sehen den Anwesenheitsstatus **Büro**.

Aktivierung

Als Teilnehmer können Sie den CallMe-Dienst manuell aktivieren. Außerdem wird der CallMe-Dienst durch Automatisches Zurücksetzen des Anwesenheitsstatus nach Abwesenheit erneut aktiviert, wenn er zuvor aktiv war. Folgende Arten von CallMe-Zielen werden nicht unterstützt:

- Gruppe
- umgeleitetes Telefon

Anzeige des CallMe-Ziels in Favoritenliste

Als Teilnehmer können Sie an Stelle Ihrer Rufnummer die Rufnummer Ihres CallMe-Ziels in der Favoritenliste anderer Teilnehmer anzeigen lassen.

Deaktivierung

Der CallMe-Dienst bleibt bis zur Änderung Ihres Anwesenheitsstatus aktiv.

12.4.3 Statusbezogene Anrufumleitung

Mit der statusbezogenen Anrufumleitung kann der Teilnehmer Anrufer auf Basis seines Anwesenheitsstatus zu einer seiner zusätzlichen Rufnummern oder zur Sprachbox umleiten.

Sie können als Teilnehmer die statusbezogene Anrufumleitung für jeden Anwesenheitsstatus außer **Büro**, **CallMe** und **Anrufschutz** konfigurieren. Wenn Sie Ihren Anwesenheitsstatus ändern, aktiviert das Kommunikationssystem die Anrufumleitung zu dem hierfür von Ihnen festgelegten Ziel, z. B. wenn Sie außer Haus sind zu Ihrem Mobiltelefon und während Ihres Urlaubs zu Ihrer Vertretung.

12.4.4 Regelbasierte Anrufumleitung

Mit der regelbasierten Anrufumleitung kann der Teilnehmer Anrufer auf Basis vielfältiger Bedingungen oder Ausnahmen noch flexibler umleiten als mit der statusbezogenen Anrufumleitung, z. B. Anrufe von unbekannten Kontakten an seine Sprachbox.

Darüber hinaus unterstützt die regelbasierte Anrufumleitung:

- beliebige Ziele
- Anwesenheitsstatus **Büro**, **CallMe** und **Anrufschutz**

Sie können als Teilnehmer mit dem Regelassistenten Regeln festlegen und jederzeit aktivieren oder deaktivieren. Eine Regel ist nur aktiv, wenn Ihr Telefon

nicht umgeleitet ist. Eine statusbezogene Anrufumleitung (außer zur Sprachbox) setzt die regelbasierte Anrufumleitung außer Kraft.

Wenn eine Regel für Anrufumleitung aktiv ist, zeigt das Display Ihres Telefons deren Namen an.

Bei einem ankommenden Anruf prüft das Kommunikationssystem die Anwendbarkeit der aktiven Regeln entsprechend ihrer Reihenfolge im Regelassistenten. Nur die erste anwendbare Regel wird ausgeführt. In diesem Fall klingelt Ihr Telefon ein Mal und anschließend leitet das Kommunikationssystem den Anruf zum festgelegten Ziel um.

Sie können in einer Regel mehrere Arten von Bedingungen und Ausnahmen (außer …) definieren. Dabei können Sie keine Bedingung zusammen mit der artverwandten Ausnahme definieren. So ist es z. B. nicht möglich eine Bedingung der Art "an bestimmten Wochentagen" zusammen mit einer Ausnahme der Art "außer an bestimmten Wochentagen" festzulegen.

Arten von Bedingungen und Ausnahmen

- (außer) bei bestimmtem Anwesenheitsstatus
- (außer) von bestimmten Personen (im internen Verzeichnis, im externen Verzeichnis, im persönlichen Verzeichnis oder von beliebiger Rufnummer)
- (außer) an Sie übergeben von bestimmten Personen (im internen Verzeichnis, im externen Verzeichnis, im persönlichen Verzeichnis oder von beliebiger Rufnummer)
- (außer) von einem bestimmten Typ, d. h. **intern**, **extern** oder **Unbekannter Kontakt**
- (außer) an einem bestimmten Datum (auch an mehreren)
- (außer) an bestimmten Wochentagen
- (außer) zwischen einem bestimmten Start- und Endedatum
- (außer) zwischen einer bestimmten Start- und Ende-Uhrzeit

12.5 Verzeichnisse und Journal (UC Suite)

Verzeichnisse, die Favoritenliste und das Journal organisieren Kontakte und Anrufe.

12.5.1 Verzeichnisse (UC Suite)

Verzeichnisse organisieren die Kontakte der Teilnehmer. Teilnehmer können mit UC Suite Clients sowie mit Systemtelefonen mit Display auf Kontakte zugreifen.

Das System bietet folgende Verzeichnisse, die folgende Funktionen unterstützen:

Verzeichnis	myPortal for Desktop, my Attendant, Fax Printer	myPortal for Outlook	Systemtelefon mit Display
Outlook-Kontakte Mac OS-Kontakte (myPortal for Desktop)	Bei Bedarf kann der Teilnehmer die Outlook-/Mac OS-Kontakte beim Start von myPortal for Desktop auf Windows importieren.	Enthält die persönlichen Outlook Kontakte eines Teilnehmers. Nur der Teilnehmer selbst hat schreibenden Zugriff auf diese Daten.	-
Persönliches Verzeichnis	Der Teilnehmer kann hier entweder beim Start von myPortal for Desktop die Outlook-Kontakte bzw. Mac OS-Kontakte importieren oder persönliche Kontakte manuell pflegen. Die Änderung importierter Kontakte ist nicht möglich.	-	-
Internes Verzeichnis	Das interne Verzeichnis von UC Smart bietet mit UC Suite zusätzliche Leistungsmerkmale. Enthält alle internen Teilnehmer und Gruppen, für welche das Anzeigen im System aktiviert ist, mit ihren eventuellen zusätzlichen Rufnummern, sofern der Teilnehmer diese für andere sichtbar macht. Interne Teilnehmer mit Systemtelefon werden mit Anwesenheitsstatus dargestellt und können per Instant Messaging kontaktiert werden. Voraussetzung für die Anzeige des Anwesenheitsstatus eines Teilnehmers ist, dass der betreffende Teilnehmer dies zulässt. Gegebenenfalls wird ein geplanter Zeitpunkt der Rückkehr angezeigt. Zusätzlich wird ein vom Teilnehmer eventuell eingegebener Informationstext angezeigt. Ein Teilnehmer hat nur lesenden Zugriff auf dieses Verzeichnis.		Enthält alle internen Teilnehmer und Gruppen für welche das Anzeigen im System aktiviert ist.
Externes Verzeichnis	Enthält Kontakte aus einem Unternehmensverzeichnis und ist durch den Administrator zu konfigurieren. Ein Teilnehmer hat nur lesenden Zugriff auf dieses Verzeichnis.		-
Öffentlicher Exchange-Ordner (nicht nutzbar mit Office 365)	Enthält die Kontakte des öffentlichen Exchange-Ordners, falls vom Administrator konfiguriert. Diese werden im Externen Verzeichnis angezeigt. Details zur Nutzung der verschiedenen Microsoft Exchange Server Versionen finden Sie im Unify Experts Wiki unter `http://wiki.unify.com/wiki/OpenScape_Business#Microsoft_Exchange_Server`.		-
Externes Offline-Verzeichnis (LDAP)	Enthält Kontakte aus dem LDAP-Unternehmensverzeichnis und ist durch den Administrator zu konfigurieren. Das Externe Offline-Verzeichnis kann nur bei der Suche genutzt werden. Der Administrator kann die Anzeige des Externen Offline-Verzeichnisses für Systemtelefone aktivieren und deaktivieren.		
Systemtelefonbuch	-		Enthält alle internen Teilnehmer und alle zentralen Kurzwahlnummern. Der Administrator kann die Anzeige eines Teilnehmers im Systemtelefonbuch aktivieren und deaktivieren.

INFO: Geben Sie Rufnummern in Verzeichnissen nach Möglichkeit stets im kanonischen Format ein.

Einfache Suche

Sie können als Teilnehmer in den Verzeichnissen nach **Vorname**, **Nachname** oder einer Rufnummer suchen. Die Verzeichnisse werden in der Reihenfolge wie in der Tabelle oben durchsucht. Die Suche ist sowohl nach ganzem Wort als auch mit unvollständigem Suchbegriff möglich, z. B. Teil einer Rufnummer. Die eingestellten Suchoptionen bleiben bis auf Weiteres erhalten. Alle verwendeten Suchbegriffe werden gespeichert. Sie können die Liste der verwendeten Suchbegriffe löschen.

Erweiterte Suche

Sie können gezielt in den Feldern **Anrede**, **Vorname**, **Nachname**, **Firma**, **Nebenstelle**, **Firmen-Rufnr.**, **Geschäftlich 1**, **Geschäftlich 2**, **Privat 1**, **Privat 2**, **Mobilrufnummer** und **E-Mail** suchen und die maximale Anzahl der Treffer begrenzen. Die moderne Oberfläche von myPortal for Desktop unterstützt die erweiterte Suche nicht.

Sortierung

Die Kontakte eines Verzeichnisses von myPortal for Desktop und myPortal for Outlook können nach einer Spalte alphanumerisch auf- oder absteigend sortiert werden. Die moderne Oberfläche von myPortal for Desktop unterstützt die Sortierung nicht.

12.5.1.1 Wie Sie Verzeichnisse für Systemtelefone konfigurieren (UC Suite)

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Sie können wählen, welche Verzeichnisse an Systemtelefonen mit Display zur Verfügung stehen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telephony Server > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **System > Display**.

4) Wählen Sie in der Aufklappliste **Telefonbuch** eine der folgenden Möglichkeiten:

- Wenn sowohl das Interne Verzeichnis als auch das Externe Offline-Verzeichnis zur Verfügung stehen soll, wählen Sie **Alle**.

- Wenn nur das Interne Verzeichnis zur Verfügung stehen soll, wählen Sie **Intern**.
- Wenn nur das Externe Offline-Verzeichnis zur Verfügung stehen soll, wählen Sie **LDAP**.
- Wenn kein Verzeichnis zur Verfügung stehen soll, wählen Sie **Nein**.

5) Klicken Sie auf **Übernehmen**.

Nächste Schritte

Wenn Sie Alle oder LDAP gewählt haben, sorgen Sie dafür, dass ein Externes Offline-Verzeichnis (LDAP) für Systemtelefone zur Verfügung steht, siehe *Wie Sie ein externes Offline-Verzeichnis (LDAP) für Systemtelefone hinzufügen*.

12.5.2 Internes Verzeichnis (UC Suite)

Das interne Verzeichnis enthält die Kontaktdetails der internen Teilnehmer des Kommunikationssystems. UC Suite Clients haben Zugriff auf das Systemtelefonbuch.

Als Administrator haben Sie uneingeschränkten Zugriff auf alle Daten im internen Verzeichnis. Als Teilnehmer können Sie aus dem internen Verzeichnis wählen.

Der Administrator kann die Anzeige für alle analogen Teilnehmer oder für analoge Teilnehmer ohne Namen deaktivieren. Teilnehmer deren Name mit - beginnt werden in letzterem Fall nicht angezeigt.

12.5.2.1 Wie Sie die Anzeige analoger Teilnehmer im internen Verzeichnis aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Applikationen > UC Suite**.

3) Klicken Sie im Menübaum auf **Server**.

4) Klicken Sie auf die Registerkarte **Allgemeine Einstellungen**.

5) Wählen Sie im Bereich **Analoge Nebenstellen** in der Aufklappliste **Modus Analoger Teilnehmer** eine der folgenden Möglichkeiten:

- Wenn alle analogen Teilnehmer im internen Verzeichnis angezeigt werden sollen, wählen Sie **Alle anzeigen**.
- Wenn nur analoge Teilnehmer mit einem Namen im internen Verzeichnis angezeigt werden sollen, wählen Sie **Nur Benannte anzeigen**.

INFO: Analoge Teilnehmer deren Name mit - beginnt werden bei dieser Einstellung nicht angezeigt.

- Wenn keine analogen Teilnehmer im internen Verzeichnis angezeigt werden sollen, wählen Sie **Nicht angezeigt**.

6) Klicken Sie auf **Speichern**.

12.5.3 Externes Verzeichnis

Das externe Verzeichnis enthält Kontakte von außerhalb des Kommunikationssystems.

Die Daten des externen Verzeichnis stehen allen Teilnehmern in allen UC Suite Clients und über Telefone mit Display zur Verfügung. Teilnehmer können aus dem externen Verzeichnis wählen. Benutzer der UC Suite Clients myAttendant und myAgent können Daten im externen Verzeichnis bearbeiten.

Import einer CSV-Datei

Als Administrator können Sie Kontakte in einer CSV-Datei in UTF-8-Kodierung vom lokalen Dateisystem oder von einer Netzwerkfreigabe in das externe Verzeichnis importieren.

Eine Kopfzeile in der CSV-Datei ermöglicht die Zuordnung der Feldnamen der CSV-Datei zu Feldern im System. Die CSV-Datei kann z. B. wie folgt aufgebaut sein:

- Kopfzeile:
  "Kunden-ID","Nachname","Vorname","Firmentelefonnummer","Firmenname"
- Datenzeile:
  "987654","Dubios","Natalie","+498977712345","Company"

Sie können beim Import Daten der CSV-Datei folgenden Feldern im System zuordnen:

- Kunden-ID
- Anrede
- Vorname
- Nachname
- Firma
- Geschäftlich
- Geschäftlich 2
- Mobilnr.
- Privat
- XMPP-ID
- Faxnr.
- E-Mail
- Stadt

Nach Bearbeitung der CSV-Vorlage muss die Datei im UTF-8 Format gespeichert werden, um den korrekten Import von eventuell vorhandenen Sonderzeichen zu gewährleisten.

Wenn Sie beim Import Daten überschreiben möchten, muss die entsprechende **Kunden-ID** identisch sein.

INFO: Eine CSV-Vorlage sowie eine Beschreibung der erforderlichen Syntax für den Import von Daten für das Externe Verzeichnis finden Sie unter **Service-Center > Dokumente > CSV-Vorlagen**.

12.5.3.1 Wie Sie eine CSV-Datei vom lokalen Dateisystem in das externe Verzeichnis importieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.
- Eine geeignete CSV-Datei in UTF-8-Kodierung mit Daten für das externe Verzeichnis liegt im lokalen Dateisystem vor.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Externes Verzeichnis** zu starten.

4) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie die CSV-Datei vom lokalen Dateisystem laden möchten, aktivieren Sie das Optionsfeld **Lokale Datei** und navigieren im Bereich **Datei-Upload** zu der CSV-Datei.
- Wenn Sie die CSV-Datei von einer Netzwerkfreigabe laden möchten, aktivieren Sie das Optionsfeld **Gemeinsames Verzeichnis** und geben Sie im Bereich **Gemeinsames Verzeichnis** die Daten für den Zugang zu der Netzwerkfreigabe ein (Name der CSV-Datei, Domänen-Name sowie Benutzername und Passwort für die Freigabe).

  Die Richtigkeit Ihrer Eingaben können Sie über **Test** verifizieren.

5) Klicken Sie im Bereich **Quelldatei** auf **Durchsuchen** und wählen Sie die gewünschte Datei aus.

6) Geben Sie im Feld **Kopfzeilen** die Anzahl der Kopfzeilen der CSV-Datei ein.

7) Geben Sie das in der CSV-Datei verwendete **Feldtrennzeichen** ein.

8) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie die bestehenden Daten des externen Verzeichnisses löschen möchten, aktivieren Sie das Kontrollkästchen **Verzeichnis vor dem Import löschen**.

- Wenn Sie die bestehenden Daten des externen Verzeichnisses nicht löschen möchten, deaktivieren Sie das Kontrollkästchen **Verzeichnis vor dem Import löschen**.

9) Wählen Sie im Bereich **Behandlung bei gleichen Kunden-IDs**, wie das System beim Importversuch von Daten mit bereits vorhandener Kunden-ID reagieren soll:

- Wenn Sie vorhandene Kontakte mit den Daten aus der CSV-Datei überschreiben möchten, wählen Sie **Kontakte aktualisieren**.
- Wenn Sie vorhandene Kontakte beibehalten möchten, wählen Sie **Vorhandene Kontakte beibehalten**.

10) Klicken Sie auf **Weiter**.

11) Wählen Sie in den Aufklapplisten der Reihe nach die Zuordnung der Felder der CSV-Datei zu den entsprechenden Feldern im System aus. Wenn die Felder nicht vorhanden sind oder Sie die Daten nicht importieren möchten, klicken Sie auf **Kein Mapping**.

12) Klicken Sie auf **Weiter**.

13) Klicken Sie auf **Importieren**. Schließen Sie dieses Fenster nicht, während der Import läuft. Nach Beenden des Imports wird die Anzahl der importierten Datensätze angezeigt.

12.5.3.2 Wie Sie Zugriff auf eine externe Datenbank für das Externe Verzeichnis hinzufügen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.
- Die Daten für den Zugriff auf die externe Datenbank liegen vor.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Externes Verzeichnis** zu starten.

4) Klicken SIe im Bereich **Quelldatei** auf **Durchsuchen** und wählen Sie die gewünschte Datei aus.

12.5.4 Externes Offline-Verzeichnis (LDAP)

Das Externe Offline-Verzeichnis (LDAP) enthält Kontakte von einem LDAP-Server für myPortal for Desktop, myAgent, Fax Printer, myPortal for Outlook und für Systemtelefone mit Display.

Das System unterstützt LDAP Version 2 mit Authentifizierung.

LDAP (Lightweight Directory Access Protocol) ist ein TCP/IP-basiertes Directory-Zugangsprotokoll für den Zugriff auf Netzwerk-Verzeichnisdienste. LDAP hat ein weltweit eindeutiges Format, in dem alle Namen darstellbar sind, es bietet unterschiedliche Layouts und eine eindeutige Zuordnung zwischen Namen und ihrer internen Repräsentation. Der Administrator definiert zusammen mit dem IT-Administrator des Kunden beim Projektgespräch diese Daten. LDAP kann unter den Betriebssystemen MS Windows und Linux verwendet werden.

In einer Microsoft-Umgebung ist der Active Directory Server (ADS) bzw. der Exchange Server auch gleichzeitig der LDAP-Server. Unter Microsoft Windows können die Benutzerdaten z. B. mit der Applikation Active Directory oder ESTOS Metadir verwaltet werden. Die Verwaltung dieser Daten erledigt im allgemeinen der IT-Administrator des Kunden.

Unter Linux können die Benutzerdaten z. B. mit OpenLDAP verwaltet werden.

Ein LDAP-Browser (z. B. Freeware von Softerra) vereinfacht die Einrichtung eines LDAP-Verzeichnisdienstes.

Rufnummern auf dem LDAP-Server dürfen als Trennzeichen nur "-" und Leerzeichen enthalten. Andere Trennzeichen kann das System nicht ausfiltern.

Bei der Konfiguration eines Externen Offline-Verzeichnisses können Sie als Administrator das Mapping der Felder an die Namen des verwendeten LDAP-Servers anpassen. Gelöschte Felder werden bei der Suche nach Namen mittels Rufnummer ignoriert. Die Suche erfolgt immer mit den letzten 4 Stellen der Rufnummer mit vorangestellter Wildcard. Sie können die Suche nach Namen mittels Rufnummer bei kommenden Gesprächen deaktivieren.

Sollte der standardmäßig verwendet Port 389 belegt sein, ist ein anderer zu konfigurieren.

INFO: Weitere Informationen finden Sie im Internet unter: `http://wiki.unify.com`.

Die Daten des externen Verzeichnis stehen Teilnehmern in myPortal for Desktop, myAttendant, Fax Printer und myPortal for Outlook bei der Suche zur Verfügung.

Systemtelefone mit Display

Als Teilnehmer können Sie im Menü zwischen dem internen Verzeichnis und dem LDAP-Verzeichnis wählen, sofern diese für Systemtelefone konfiguriert sind. Das LDAP-Verzeichnis unterstützt die Suche in den entsprechenden Kontakten und den anschließenden Anruf eines Kontakts.

Die vom LDAP-Server bereitgestellte Namensinformation wird nicht für die Displayanzeige im Ruf- oder Gesprächszustand verwendet. Die Rufnummern kommender Rufe werden ebenfalls nicht durch die vom LDAP-Server bereitgestellten Namensinformationen ersetzt (wie beispielsweise bei der Ersetzung von Rufnummern durch KWZ-Namen).

Ein Teilnehmer des Systems ist nur dann aus dem LDAP-Verzeichnis erreichbar, wenn für ihn eine Durchwahlrufnummer konfiguriert wurde und diese mit dem Eintrag in der LDAP-Datenbank übereinstimmt. Vom LDAP-Server bereitgestellte

Rufnummern können nur dann netzintern geroutet werden, wenn interne Rufnummer und Durchwahlrufnummer identisch sind.

12.5.4.1 Wie Sie ein externes Offline-Verzeichnis (LDAP) für PC-Clients hinzufügen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.
- Ihnen liegen die Zugangsdaten für den LDAP-Server vor.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Applikationen > UC Suite**.

3) Klicken Sie auf die Registerkarte **Konfiguration externe Anbieter**.

4) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie im Journal für externe ankommende Anrufe die Auflösung von Rufnummern in Namen aktivieren möchten, aktivieren Sie das Kontrollkästchen **Suchen nach Rufnummer**.
- Wenn Sie im Journal für externe ankommende Anrufe die Auflösung von Rufnummern in Namen deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Suchen nach Rufnummer**.

5) Klicken Sie auf **Hinzufügen**.

6) Geben Sie die Zugangsdaten des LDAP-Servers ein:

a) Geben Sie in **Name** einen Namen für dieses Externe Offline-Verzeichnis ein.

b) Geben Sie in **Server** den Namen oder die IP-Adresse des LDAP-Servers ein.

c) Geben Sie in **Port** die Portnummer des LDAP-Servers ein.

d) Geben Sie in **LDAP Basis-DN** den LDAP Base Distinguished Name ein, z. B. `dc=example-for-a-domain, dc=net`.

e) Geben Sie **Benutzername** ein.

f) Geben Sie das **Kennwort** ein.

7) Geben Sie in die Felder bei **Anrede**, **Vorname**, **Nachname**, **Geschäftlich 1**, **Geschäftlich 2**, **Privat**, **Mobil**, **Firma**, **Firmen-Rufnr.**, **Postanschrift**, **Bundesland oder Region**, **Land**, **Postleitzahl**, **E-Mail**, **Pager**, **Faxrufnummer**, **XMPP-ID** und **Stadt** jeweils die entsprechende Feldbezeichnung des LDAP-Servers ein.

8) Klicken Sie auf **Speichern**.

12.5.4.2 Wie Sie ein externes Offline-Verzeichnis (LDAP) für PC-Clients löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Applikationen > UC Suite**.

3) Klicken Sie auf die Registerkarte **Konfiguration externe Anbieter**.

4) Klicken Sie auf das zu löschende Externe Offline-Verzeichnis.

5) Klicken Sie auf **Entfernen**.

12.5.4.3 Wie Sie ein externes Offline-Verzeichnis (LDAP) für Systemtelefone hinzufügen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.
- Ihnen liegen die Zugangsdaten für den LDAP-Server vor.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telephony Server > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **System > LDAP**.

4) Geben Sie die **IP-Adresse des LDAP-Servers** ein.

5) Geben Sie die **Portnummer des LDAP-Zugangs** ein.

6) Geben Sie **Benutzername** ein.

7) Geben Sie das **Kennwort** ein.

8) Geben Sie in **Kennwort bestätigen** das Kennwort ein.

9) Geben Sie in **Basis DN** den LDAP BASE Distinguished Name des LDAP-Servers ein, z. B. `dc=example-for-a-domain, dc=net`.

10) Geben Sie in **Suchanfrage** den Suchstring für den LDAP-Server ein, z. B. `cn=$*`.

11) Geben Sie **Ergebnisattribut Name** für den LDAP-Server ein, z. B. `cn`.

12) Geben Sie **Ergebnisattribut Rufnummer** für den LDAP-Server ein, z. B. `telephoneNumber`.

13) Wählen Sie für die Sortierung der Suchergebnisse eine der folgenden Möglichkeiten:

- Wenn Sie die Suchergebnisse sortiert haben möchten, aktivieren Sie das Kontrollkästchen **Sortieren der Suchergebnisse**.
- Wenn Sie die Suchergebnisse nicht sortiert haben möchten, deaktivieren Sie das Kontrollkästchen **Sortieren der Suchergebnisse**.

14) Geben Sie die **LDAP-Belegungskennzahl** ein.

15) Geben Sie das **LDAP-Rufnummernprefix** ein.

16) Klicken Sie auf **Übernehmen**.

Nächste Schritte

Wie Sie Verzeichnisse für Systemtelefone konfigurieren (UC Suite)

12.5.5 Systemtelefonbuch (UC Suite)

Das Systemtelefonbuch enthält alle internen Teilnehmer und alle zentralen Kurzwahlnummern für welche jeweils ein Name vergeben wurde. UC Suite Clients haben Zugriff auf das Systemtelefonbuch.

Der Administrator kann die Anzeige für jeden Teilnehmer bzw. jede Kurzwahlnummer mit Namen individuell deaktivieren.

12.5.6 Abteilungen

Abteilungen gruppieren Teilnehmer im internen Verzeichnis nach ihrer organisatorischen Zugehörigkeit. Das interne Verzeichnis ermöglicht die Suche bzw. Sortierung nach Abteilung.

12.5.6.1 Wie Sie eine Abteilung hinzufügen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Abteilungen** zu starten.

4) Klicken Sie auf **Hinzufügen**.

5) Geben Sie **Name** der Abteilung ein.

6) Geben Sie die **Gruppennummer** ein.

7) Klicken Sie auf **Speichern**.

12.5.6.2 Wie Sie Teilnehmer einer Abteilung zuordnen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Benutzerverzeichnis** zu starten.

4) Wählen Sie den betreffenden Teilnehmer aus.

5) Klicken Sie auf **Bearbeiten**.

6) Wählen Sie im Feld **Abt.** aus der Aufklappliste die gewünschte Abteilung aus.

7) Klicken Sie anschließend auf **Speichern**.

12.5.6.3 Wie Sie eine Abteilung bearbeiten

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Abteilungen** zu starten.

4) Klicken Sie in der Liste der Abteilungen auf die entsprechende Abteilung.

5) Klicken Sie auf **Bearbeiten**.

6) Geben Sie **Name** der Abteilung ein.

7) Geben Sie die **Gruppennummer** ein.

8) Klicken Sie auf **Speichern**.

12.5.6.4 Wie Sie eine Abteilung entfernen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Abteilungen** zu starten.

4) Klicken Sie in der Liste der Abteilungen auf die entsprechende Abteilung.

5) Klicken Sie auf **Entfernen**.

6) Klicken Sie auf **OK**.

12.5.7 Favoritenliste

In der Favoritenliste haben Sie als Teilnehmer ausgewählte Kontakte stets im Blick. Diese können Sie besonders einfach anrufen. Alle internen Teilnehmer mit Systemtelefon sowie externe XMPP-Kommunikationspartner sehen Sie mit Anwesenheitsstatus und können diese per Sofortnachricht kontaktieren.

Sie können als Teilnehmer Kontakte aus allen Verzeichnissen zur Favoritenliste hinzufügen. Bei Favoriten, die nicht aus dem internen Verzeichnis stammen, erscheint an Stelle des Symbols für den Anwesenheitsstatus das Symbol für die Quelle des Kontakts.

Die Favoritenliste verwaltet Kontakte in Gruppen. Die Kontakte in allen Gruppen sind nach Vorname, Nachname oder in ihrer ursprünglichen Reihenfolge sortierbar.

Bei Abwesenheit eines internen Teilnehmers erfahren Sie den geplanten Zeitpunkt der Rückkehr durch Positionieren des Mauszeigers auf seinem Eintrag, sofern er seinen Anwesenheitsstatus für Sie sichtbar sein lässt.

Bei Favoriten mit mehreren Rufnummern können Sie eine Standard-Rufnummer festlegen, unter welcher der Kontakt angerufen wird. Die Standard-Rufnummer eines Favoriten ist im Kontextmenü am Symbol mit dem aktivierten Kontrollkästchen erkennbar.

12.5.8 Journal (UC Suite)

Das Journal ist die Liste aller ankommenden und gehenden Anrufe eines Teilnehmers. Aus dem Journal kann der Teilnehmer Kontakte schnell und einfach erneut anrufen oder entgangene Anrufe beantworten.

Ordner für Anrufarten

Die Anrufe sind in folgende Gruppen gegliedert:

- **Offen**
  Enthält unbeantwortete entgangene Anrufe, bei denen eine Rufnummer übermittelt wurde. Sobald einer dieser Anrufe beantwortet wird, entfallen alle Einträge mit der entsprechenden Rufnummer.
- **Alle Anrufe**

- **Entgangen**
- **Angenommen**
- **Intern**
- **Extern**
- **Ankommend**
- **Gehend**
- **Geplant**
  Enthält die von Ihnen als Teilnehmer zu bestimmten Terminen geplanten Anrufe. Das Leistungsmerkmal Geplante Anrufe steht für Agenten von Contact Center nicht zur Verfügung. Damit das Kommunikationssystem einen geplanten Anruf ausführt, muss zu dem Termin myPortal for Desktop oder myPortal for Outlook geöffnet sein, der Anwesenheitsstatus muss **Büro** oder **CallMe** sein und Sie müssen die Ausführung des Anrufs in einem Dialog bestätigen. Falls Sie während des Termins für einen geplanten Anruf besetzt sind, stellt das System den geplanten Anruf zurück bis Sie wieder frei sind. myPortal for Desktop oder myPortal for Outlook weist Sie beim Beenden auf eventuell anstehende geplante Anrufe hin. Beim Starten informiert myPortal for Desktop oder myPortal for Outlook Sie über eventuell inzwischen verstrichene Termine geplanter Anrufe. Sie können diese dann entweder löschen oder zu einem neuen Termin speichern.

In der modernen Benutzeroberfläche von myPortal for Desktop stehen nicht alle Ordner für Anrufarten zur Verfügung.

Aufbewahrungsdauer

Das System speichert Anrufe im Journal für eine begrenzte, vom Administrator konfigurierbare maximale Zeit. Als Teilnehmer können Sie diese Zeit reduzieren. Nach Ablauf der Aufbewahrungsdauer löscht das System betreffende Einträge automatisch.

> ***INFO:*** Die Aufbewahrungsdauer legt auch den maximalen Zeitraum für Auswertungen mit myReports fest.

Gruppierung nach Zeitraum

Die Anrufe sind in jeder Gruppe zeitlich gruppiert, z. B.: Heute, Gestern, etc., Letzte Woche, Letzten Monat und Älter. Ihr Administrator kann einstellen, wie lange Anrufe im Journal gespeichert bleiben. Nach der eingestellten Zeit werden Einträge automatisch gelöscht. In der modernen Benutzeroberfläche von myPortal for Desktop steht die Gruppierung nach Zeitraum nicht zur Verfügung.

Anrufdetails

Jeder Anruf wird mit Datum und Uhrzeit angezeigt und sofern vorhanden mit der Rufnummer. Falls ein Verzeichnis zur Rufnummer weitere Informationen enthält wie **Nachname**, **Vorname** und **Firma**, werden auch diese angezeigt. Zusätzlich angezeigt werden in den meisten Ordnern **Richtung**, **Dauer** und die Spalte **Gespräch abgeschlossen**. In der modernen Benutzeroberfläche von myPortal for Desktop stehen nicht alle Anrufdetails zur Verfügung.

Sortierung

Sie können die Anrufe im Journal nach einer Spalte alphanumerisch auf- oder absteigend sortieren.

Sie können im Journal zum ersten Anruf springen, dessen Eintrag in der Spalte, nach der sortiert ist, mit einem bestimmten Zeichen beginnt, z. B. zum ersten Nachnamen, der mit "P" beginnt. Durch die Eingabe nachfolgender Zeichen können Sie sich gewünschten Treffern nähern. In der modernen Benutzeroberfläche von myPortal for Desktop steht die Sortierung nicht zur Verfügung.

Export

Als Teilnehmer können Sie das Journal mit myPortal for Desktop oder mit myPortal for Outlook als CSV-Datei exportieren.

12.5.8.1 Wie Sie die maximale Aufbewahrungsdauer für das Journal ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Applikationen > OpenScape Business UC Suite**.

3) Klicken Sie auf **Server**.

4) Klicken Sie auf **Wartung**.

5) Geben Sie im Feld **Anrufhistorie aufbewahren für** die gewünschte Dauer in Tagen ein.

> ***INFO:*** Die Aufbewahrungsdauer legt auch den maximalen Zeitraum für Auswertungen mit myReports fest.

6) Klicken Sie auf **Speichern**.

12.6 Anrufe (UC Suite)

Für Anrufe stehen Teilnehmern komfortable Leistungsmerkmale wie Desktop-Wahl, PopUp-Fenster und die Aufzeichnung von Anrufen und Konferenzen zur Verfügung.

12.6.1 Desktop-Wahl und Clipboard-Wahl

Desktop-Wahl und Clipboard-Wahl ermöglicht Teilnehmern mit myPortal for Desktop (Windows) oder myPortal for Outlook aus vielen Windows-Anwendungen ein markiertes Ziel bzw. ein Ziel in der Windows-Zwischenablage mittels Tastenkombination anzurufen, z. B. aus einer Outlook-E-Mail.

Abhängig von der Art der verwendeten Zeichenfolge funktioniert die Wahl folgendermaßen:

- Eine Rufnummer im kanonischen Format wird gewählt.
- Eine Rufnummer im wählbaren Format wird gewählt, sofern das Kommunikationssystem entscheiden kann, ob es sich um ein internes oder externes Ziel handelt. Anderenfalls wird der Benutzer zur entsprechenden Auswahl aufgefordert.
- Eine Zeichenfolge, die Buchstaben enthält, wird in den Verzeichnissen als Vorname oder Nachname gesucht.

Die Desktop-Wahl und Clipboard-Wahl wird nach einer einstellbaren Zeit ausgeführt. Innerhalb dieser Zeitspanne können Sie die Wahl noch abbrechen. Ändern Sie den voreingestellten Wert von 3s auf 0s wird die Wahl sofort ausgeführt.

Windows-Anwendungen, die mittels Windows-Standardkomponenten implementiert wurden, unterstützen in der Regel Desktop-Wahl und Clipboard-Wahl, nicht jedoch 16-bit-Anwendungen.

12.6.2 PopUp-Fenster

PopUp-Fenster in den UC Suite Clients bieten Teilnehmern die komfortable Möglichkeit mit einem Klick zu reagieren, z. B. auf ankommende Anrufe oder neue Sprachnachrichten.

PopUp-Fenster werden in der unteren rechten Ecke des Bildschirms angezeigt. Es gibt unterschiedliche Arten von PopUp-Fenstern. PopUp-Fenster für Anrufe und Nachrichten zeigen Rufnummer, Name und Bild des Anrufers an, wenn möglich. Die Schaltflächen der PopUp-Fenster ändern sich situationsbezogen.

PopUp-Fenster können zu einem Taskleistensymbol minimiert werden. Sobald mehr als drei PopUp-Fenster für Anrufe geöffnet sind, werden diese automatisch minimiert in der Taskleiste dargestellt.

12.6.3 Aufzeichnen von Anrufen

Ein Teilnehmer kann Anrufe aufzeichnen. Aufgezeichnete Anrufe erscheinen in der Sprachbox.

INFO: Sie müssen Ihre Gesprächspartner darüber informieren, dass Sie das Gespräch aufzeichnen. In bestimmten Ländern

(z. B. Frankreich) informiert das System den Gesprächspartner automatisch darüber.

Als Administrator können Sie das Aufzeichnen von Anrufen zusammen mit dem Aufzeichnen von Konferenzen systemweit zulassen oder verhindern. Optional können Sie zu Beginn der Aufzeichnung die Wiedergabe einer Ansage oder eines Hinweistons konfigurieren.

Als Teilnehmer können Sie das Aufzeichnen von Anrufen über myPortal for Desktop oder myPortal for Outlook steuern. Aufgezeichnete Anrufe sind in der Sprachbox durch einen roten Punkt gekennzeichnet und zeigen, sofern verfügbar, die Rufnummer des Gesprächspartners.

Durch Rückfrage, Halten, Übergabe oder Einleiten einer Konferenz wird eine laufende Aufzeichnung abgebrochen.

12.6.3.1 Wie Sie das Aufzeichnen von Anrufen aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Applikationen > OpenScape Business UC Suite**.

3) Klicken Sie auf **Server**.

4) Klicken Sie auf **Allgemeine Einstellungen**.

5) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie das Aufzeichnen von Anrufen und das Aufzeichnen von Konferenzen zulassen möchten, aktivieren Sie das Kontrollkästchen **Gespräch aufzeichnen**.
- Wenn Sie das Aufzeichnen von Anrufen und das Aufzeichnen von Konferenzen verhindern möchten, deaktivieren Sie das Kontrollkästchen **Gespräch aufzeichnen**.

6) Klicken Sie auf **Speichern**.

12.6.3.2 Wie Sie eine Ansage für Aufzeichnung aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen > OpenScape Business UC Suite**.
3) Klicken Sie auf **Server**.
4) Klicken Sie auf **Allgemeine Einstellungen**.
5) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie zu Beginn einer Aufzeichnung eine Ansage wiedergeben möchten, aktivieren Sie das Kontrollkästchen **Vor der Aufzeichnung eine Ansage wiedergeben**.
   - Wenn Sie zu Beginn einer Aufzeichnung keine Ansage wiedergeben möchten, deaktivieren Sie das Kontrollkästchen **Vor der Aufzeichnung eine Ansage wiedergeben**.
6) Klicken Sie auf **Speichern**.

12.6.3.3 Wie Sie den Hinweiston für eine Aufzeichnung aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen > OpenScape Business UC Suite**.
3) Klicken Sie auf **Server**.
4) Klicken Sie auf **Allgemeine Einstellungen**.
5) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie zu Beginn einer Aufzeichnung einen Hinweiston wiedergeben möchten, aktivieren Sie das Kontrollkästchen **Vor der Aufzeichnung einen Hinweiston wiedergeben**.
   - Wenn Sie zu Beginn einer Aufzeichnen keinen Hinweiston wiedergeben möchten, deaktivieren Sie das Kontrollkästchen **Vor der Aufzeichnung einen Hinweiston wiedergeben**.
6) Klicken Sie auf **Speichern**.

12.7 Konferenzen (UC Suite)

In einer Konferenz können mehrere Teilnehmer (darunter auch externe) gleichzeitig miteinander telefonieren.

12.7.1 Konferenzmanagement

Mit Konferenzmanagement kann ein Teilnehmer unterschiedliche Arten von Konferenzen nutzen.

Arten von Konferenzen

Die unterschiedlichen Arten von Konferenzen bieten folgende Möglichkeiten:

	Ad-hoc	geplant	permanent	offen
Nutzung	• telefongesteuert • applikationsgesteuert	• applikationsgesteuert	• applikationsgesteuert	• applikationsgesteuert
Start	• manuell	• nach Zeitplan	• manuell	• manuell
Ende	• manuell	• nach Zeitplan • manuell	• manuell	• manuell
Dauer der Reservierung von Konferenzkanälen	• standardmäßig 1 Stunde	• nach Zeitplan	• bis zur Deaktivierung oder Löschung der Konferenz	• bis zur Deaktivierung oder Löschung der Konferenz
Verlängerung	x	x	-	-
Wiederholung	• manuell	• nach Zeitplan	-	-
Richtung des Verbindungsaufbaus aus Sicht des Systems	• gehend	• gehend • ankommend	• ankommend	• ankommend
Teilnehmerkreis	• fest	• fest	• fest	• offen
Authentifizierung der Konferenzteilnehmer	-	• individuelle Konferenz-ID (optional) • Kennwort (optional)	• individuelle Konferenz-ID (optional) • Kennwort (optional)	• gemeinsame Konferenz-ID (optional)

	Ad-hoc	geplant	permanent	offen
Aufzeichnung, sofern im System aktiviert	• manuell (On Demand Conference Recording)	• automatisch (Auto Conference Recording) • manuell (On Demand Conference Recording)	• automatisch (Auto Conference Recording) • manuell (On Demand Conference Recording)	• automatisch (Auto Conference Recording) • manuell (On Demand Conference Recording)
Einladung per E-Mail mit:	• Name der Konferenz • Link für Web Collaboration Sitzung	• Name der Konferenz • Einwahlnummer • Konferenz-ID • Kennwort • Datum und Uhrzeit von Beginn und Ende der Konferenz • Link für Web Collaboration Sitzung	• Name der Konferenz • Einwahlnummer • Konferenz-ID • Kennwort • Link für Web Collaboration Sitzung	• Name der Konferenz • Einwahlnummer • Konferenz-ID • Kennwort
Outlook-Termin als E-Mail-Anlage (.ics)	-	x	-	-

Applikationsgesteuerte Konferenz

Als Teilnehmer können Sie eine Konferenz mit dem Konferenz-Management von myPortal for Desktop oder myPortal for Outlook initiieren, steuern und verwalten.

Telefongesteuerte Konferenz

Als Teilnehmer können Sie eine telefongesteuerte Konferenz auf folgende Arten initiieren und anschließend am Telefon steuern:

- gewünschte Konferenzteilnehmer anrufen und mit der Konferenz verbinden
- Rückfrageverbindung zu einer Konferenz erweitern
- Zweitanruf zu einer Konferenz erweitern

Virtueller Konferenzraum

Im virtuellen Konferenzraum können Sie als Teilnehmer bei applikationsgesteuerten Konferenzen in Echtzeit eine Konferenz mit ihrem Teilnehmerkreis grafisch dargestellt verfolgen und als Konferenzleiter auch steuern. Der virtuelle Konferenzraum zeigt Rufnummer, Name und Anwesenheitsstatus der Konferenzteilnehmer an, sofern verfügbar.

Einwahlnummer

Als Administrator können Sie die bei der Basisinstallation festgelegten Einwahlnummern für Konferenzen ändern. Als Teilnehmer können Sie die Einwahlnummer für eine Konferenz anzeigen.

Konferenzleiter

Der Initiator der Konferenz ist bis auf Weiteres automatisch Konferenzleiter. Dieser kann (abhängig von der Art der Konferenz):

- Konferenzteilnehmer hinzufügen oder entfernen (applikationsgesteuerte Konferenz):
  Entfernte Teilnehmer bleiben nicht in der Konferenz.
- Konferenzteilnehmer trennen oder erneut verbinden:
  Getrennte Teilnehmer können weiterhin in der Konferenz bleiben. Während der Konferenzleiter einen Konferenzteilnehmer verbindet, hört der einzige andere Konferenzteilnehmer Wartemusik bzw. bleiben die anderen Konferenzteilnehmer miteinander verbunden.
- die Konferenz aufzeichnen
  Aufgezeichnete Konferenzen erscheinen in der Sprachbox mit einem roten Punkt gekennzeichnet und zeigen, sofern verfügbar, die Rufnummer des ersten Konferenzteilnehmers. Konferenzen, an denen ein gehaltener Teilnehmer beteiligt ist, können nicht aufgezeichnet werden.
- einen anderen internen Teilnehmer desselben Knotens als Konferenzleiter festlegen
- die Konferenz verlängern
- die Konferenz verlassen, ohne sie zu beenden:
  Der am längsten teilnehmende interne Teilnehmer wird automatisch Konferenzleiter.
- die Konferenz beenden

Konferenzteilnehmer

Konferenzteilnehmer können die Konferenz verlassen oder sich erneut einwählen (geplante Konferenz und permanente Konferenz). Solange eine Konferenz nur einen Teilnehmer hat, hört dieser Wartemusik. Als Administrator können Sie festlegen, ob in Konferenzen mehrere externe Konferenzteilnehmer zulässig sind. Die maximale Anzahl der externen Konferenzteilnehmer ist unter anderem durch die Anzahl der verfügbaren Amtsleitungen begrenzt.

Konferenzton

Beim Verbinden oder Trennen eines Konferenzteilnehmers hören die anderen Konferenzteilnehmer den Konferenzton. Als Administrator können Sie den Konferenzton aktivieren oder deaktivieren.

Automatisches Beenden ohne Konferenzleiter

Verbleiben in einer Konferenz nur externe Teilnehmer, hören die Konferenzteilnehmer nach Ablauf einer bestimmten Zeit einen Aufmerksamkeitston. Nach Ablauf einer weiteren Zeit beendet das System die Konferenz automatisch. Als Administrator können Sie diese Zeiten ändern.

Benachrichtigung per E-Mail und Outlook-Termin

Das System kann Konferenzteilnehmer automatisch per E-Mail und bei geplanten Konferenzen zusätzlich mittels Outlook-Termin als Anlage (.ics) benachrichtigen:

Ereignis	benachrichtigte Konferenzteilnehmer	Outlook-Termin
Neue Konferenz	alle	automatische Erstellung
Löschen der Konferenz		automatische Löschung
Verschieben der Konferenz		automatische Aktualisierung
Hinzufügen von Konferenzteilnehmern	betroffene	automatische Erstellung (betroffene)
Entfernen von Konferenzteilnehmern		automatische Löschung (betroffene)

Voraussetzung ist, dass der Administrator den E-Mail-Versand konfiguriert hat. Ferner muss ein interner Konferenzteilnehmer seine E-Mail-Adresse festgelegt haben. Für externe Konferenzteilnehmer muss der Initiator der Konferenz deren E-Mail-Adresse eingeben.

INFO: Zur Benachrichtigung per E-Mail erfolgt keinerlei Rückmeldung über fehlgeschlagene Zustellung oder über eventuelle Abwesenheitsmitteilungen, da E-Mails wegen der Integration von Web Collaboration direkt vom System gesendet werden.

Weitere Anrufe

Während der Teilnahme an einer Konferenz führt das Ausführen oder das Annehmen eines anderen Anrufs zur Trennung von der Konferenz.

Parken, Makeln

In einer Konferenz stehen die Leistungsmerkmale Parken und Makeln nicht zur Verfügung.

Gebühren

Gebühren werden demjenigen Teilnehmer zugeordnet, der das gebührenpflichtige Gespräch aufgebaut hat. Mit Übergabe an einen anderen Konferenzleiter gehen die weiteren Gebühren auf diesen über.

Systemauslastung

Als Administrator können Sie sowohl aktive als auch gespeicherte Konferenzen anzeigen. Inaktive Konferenzen können gelöscht werden.

INFO: Permanente Konferenzen belegen dauerhaft Systemressourcen. Da jeder Teilnehmer mit myPortal for Desktop oder myPortal for Outlook permanente Konferenzen konfigurieren kann, empfehlen wir Ihnen als Administrator regelmäßig die gespeicherten Konferenzen zu überprüfen, um Ressourcenengpässe zu vermeiden.

Videoübertragung

Eine eventuell laufende Videoübertragung muss vor der Teilnahme an einer Konferenz beendet werden.

12.7.1.1 Wie Sie die Einwahlnummer für einen virtuellen Konferenzraum ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telephonie > Teilnehmer**.

3) Navigieren Sie im Menübaum zu **Teilnehmer > Applikation-Suite > Konferenz**.

Im Arbeitsbereich werden die Rufnummern der virtuellen Konferenzräume angezeigt. Die letzte davon ist jene für geplante Konferenzen und permanente Konferenzen.

4) Klicken Sie im Menübaum auf den betreffenden Eintrag (Index - Rufnummer).

5) Klicken Sie auf die Registerkarte **Teilnehmer-Parameter ändern**.

6) Geben Sie im Feld **Rufnummer** die neue Einwahlnummer ein. Die Einwahlnummer darf nur die Ziffern 0-9 enthalten.

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

12.7.1.2 Wie Sie mehrere externe Konferenzteilnehmer zulassen oder verhindern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Navigieren Sie im Menübaum zu **System > System Flags**.

4) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie mehrere externe Konferenzteilnehmer zulassen möchten, aktivieren Sie das Kontrollkästchen **Mehr als 1 externer Konferenzteilnehmer**.
- Wenn Sie mehrere externe Konferenzteilnehmer verhindern möchten, deaktivieren Sie das Kontrollkästchen **Mehr als 1 externer Konferenzteilnehmer**.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

12.7.1.3 Wie Sie den Konferenzton aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Navigieren Sie im Menübaum zu **System > System Flags**.

4) Wählen Sie eine der folgenden Möglichleiten:

- Wenn Sie den Konferenzton aktivieren möchten, aktivieren Sie das Kontrollkästchen **Konferenzton**.
- Wenn Sie den Konferenzton deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Konferenzton**.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

12.7.1.4 Wie Sie die Zeitspanne für automatisches Beenden von Konferenzen ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Navigieren Sie im Menübaum zu **System > Zeitparameter**.

4) Wählen Sie in der Zeile bei **Zeit bis zum Aufmerksamkeitston bei HKZ-Transit-Verbindungen** in **Basis** und **Faktor** die gewünschte Zeit vom Verlassen der Konferenz durch den letzten Konferenzleiter bis zum Aufmerksamkeitston.

5) Wählen Sie in der Zeile bei **Zeit vom Aufmerksamkeitston bis zum Auslösen...** die gewünschte Zeit vom Aufmerksamkeitston bis zum automatischen Beenden der Konferenz.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

12.7.1.5 Wie Sie Details zu einer gespeicherten Konferenz abfragen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Konferenzschaltung** zu starten.
4) Klicken Sie auf die betreffende Konferenz.
5) Klicken Sie auf **Anzeige**.

12.7.1.6 Wie Sie eine gespeicherte Konferenz löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Konferenzschaltung** zu starten.
4) Klicken Sie auf die betreffende Konferenz.
5) Klicken Sie auf **Löschen** und bestätigen Sie die Sicherheitsabfrage.

12.7.1.7 Wie Sie das Aufzeichnen von Konferenzen konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen > OpenScape Business UC Suite**.
3) Klicken Sie auf **Server**.
4) Klicken Sie auf **Gespräch aufzeichnen**.
5) Wenn Sie das Aufzeichnen von Anrufen und Konferenzen zulassen möchten, aktivieren Sie das Kontrollkästchen **Gespräch aufzeichnen**. Die beiden nachfolgend beschriebenen Kontrollkästchen werden aktivierbar.

6) Wenn vor dem Aufzeichnen von Anrufen und Konferenzen eine entsprechende Ansage wiedergegeben werden soll, aktivieren Sie das Kontrollkästchen **Vor der Aufzeichnung eine Ansage wiedergeben**.

7) Wenn während des Aufzeichnens von Anrufen und Konferenzen ein Hinweiston wiedergegeben werden soll, aktivieren Sie das Kontrollkästchen **Während der Aufzeichnung einen Hinweiston wiedergeben**.

8) Klicken Sie auf **Speichern**.

12.7.2 Ad-hoc-Konferenz (UC Suite)

Eine Ad-hoc-Konferenz findet spontan statt. Der Konferenzleiter startet sie manuell. Der Konferenzleiter kann Ad-hoc-Konferenzen speichern, um sie zu einem beliebigen Zeitpunkt erneut einzuberufen.

Start der Konferenz

Das System öffnet bei allen internen Konferenzteilnehmern automatisch das Fenster mit dem virtuellen Konferenzraum, sofern der Konferenzteilnehmer myPortal for Desktop mit der klassischen Benutzeroberfläche oder myPortal for Outlook gestartet hat. Das System ruft alle Konferenzteilnehmer gleichzeitig an. Bei Eintritt in die Konferenz erhalten die Konferenzteilnehmer eine Begrüßungsansage, welche den Konferenzleiter nennt.

Aufzeichnen der Konferenz

Der Konferenzleiter kann die Konferenz manuell für sich und für alle verbundenen internen Konferenzteilnehmer aufzeichnen, sofern das Aufzeichnen von Gesprächen im System aktiviert ist. Teilnehmer des eigenen Knotens erhalten die Aufzeichnung in der Sprachbox, Teilnehmer an anderen Knoten per E-Mail. Die Dauer der Aufzeichnung ist nur durch die verfügbare Speicherkapazität des Systems begrenzt.

Beenden der Konferenz

Der Konferenzleiter kann die Konferenz im Client beenden oder durch Auflegen. Alternativ wird die Konferenz beendet, wenn alle Konferenzteilnehmer die Konferenz verlassen haben.

Erweitern eines Gesprächs zu einer Konferenz

Ein sich im Gespräch befindlicher interner Teilnehmer kann das Gespräch in eine Ad-hoc-Konferenz überführen und weitere Teilnehmer dazunehmen. Dafür muss der Teilnehmer eine UC Suite Conference Lizenz besitzen.

12.7.3 Geplante Konferenz

Eine geplante Konferenz (Meet-Me-Konferenz) findet zu einem vorher festgelegten Termin mit festgelegter Dauer statt, eventuell wiederkehrend zur selben Uhrzeit.

Eine geplante Konferenz bleibt während des gesamten geplanten Zeitraums aktiv, unabhängig davon, ob Teilnehmer verbunden sind. Der Konferenzleiter speichert eine geplante Konferenz unter einem eigenen Namen.

Optionen beim Konfigurieren einer geplanten Konferenz

Der Initiator der Konferenz kann folgende Eigenschaften festlegen:

- Beginn- und Ende-Zeitpunkt
- regelmäßig stattfindend
- Anwesenheit des Konferenzleiters erforderlich
- Authentifizierung der Konferenzteilnehmer beim Eintreten in die Konferenz erforderlich (durch Eingabe von Konferenz-ID und Kennwort über die Telefontastatur).

  INFO: Mobility-Entry-Teilnehmer müssen vor ihrer Authentifizierung die Kennzahl für MFV-Nachwahl eingeben.

  Das Standardkennwort für Konferenzen ist 123456. Der Konferenzleiter kann dies für Konferenzteilnehmer individuell ändern.
- Sprache der Ansagen zu Konferenzbeginn
- Richtung des Verbindungsaufbaus für jeden einzelnen Konferenzteilnehmer (Standard: **Gehend**)

Starten der Konferenz

Das System öffnet zum geplanten Zeitpunkt bei allen internen Konferenzteilnehmern automatisch das Fenster mit dem virtuellen Konferenzraum, sofern der Konferenzteilnehmer myPortal for Desktop mit der klassischen Benutzeroberfläche oder myPortal for Outlook gestartet hat. Ist die Anwesenheit des Konferenzleiters erforderlich, ruft das System zunächst diesen an und erst nach seiner erfolgreichen Authentifizierung gleichzeitig alle weiteren Konferenzteilnehmer. Konferenzteilnehmer, die zur Sprachbox umgeleitet haben oder deren Anwesenheitsstatus signalisiert, dass sie abwesend sind, werden nicht gerufen. Je nach konfiguriertem Verbindungsaufbau ruft das System die Konferenzteilnehmer an oder diese können sich selbst einwählen. Das System kündigt jeden hinzukommenden Teilnehmer mittels Ansage namentlich an: "`â€¦ nimmt an der Konferenz teil.`", vorausgesetzt der Initiator hat seine Namensansage aufgezeichnet.

INFO: Damit die Teilnehmer einer geplanten Konferenz ohne Authentifizierung zu Konferenzbeginn die Ansage mit dem Namen des Konferenzleiters hören, muss dieser zuvor einmal eine Konferenz mit Authentifizierung initiiert haben.

Einwahl

Mittels Einwahlnummer kann sich jeder Konferenzteilnehmer innerhalb des geplanten Zeitraums in die Konferenz einwählen, unabhängig von der für ihn festgelegten Richtung des Verbindungsaufbaus. Bei Einwahl außerhalb des

geplanten Zeitraums erfolgt eine entsprechende Ansage. Bei Einwahl über einen ITSP muss dieser RFC 2833 (DTMF-Zeichen) unterstützen.

Erzwingen der Authentifizierung mit *-Taste

Der Konferenzleiter kann die Konferenz so konfigurieren, dass sich jeder Konferenzteilnehmer zumindest durch Drücken der *-Taste authentifizieren muss. Dies gewährleistet, dass nur anwesende Teilnehmer mit der Konferenz verbunden werden, jedoch keine Sprachbox.

Verlängerung der Konferenz

Zehn Minuten vor dem geplanten Konferenzende hören die Konferenzteilnehmer eine Ansage mit dem Hinweis auf das baldige Konferenzende und auf eine mögliche Verlängerung durch Wahl einer bestimmten Ziffer. Ein beliebiger Konferenzteilnehmer kann die Konferenz dann durch Wahl der entsprechenden Ziffer verlängern. Der Konferenzleiter kann die Konferenz in myPortal for Outlook zu einem beliebigen Zeitpunkt verlängern.

Aufzeichnen der Konferenz

Der Konferenzleiter kann die Konferenz automatisch oder manuell für sich und für alle verbundenen internen Konferenzteilnehmer aufzeichnen, sofern das Aufzeichnen von Gesprächen im System aktiviert ist. Teilnehmer des eigenen Knotens erhalten die Aufzeichnung in der Sprachbox, Teilnehmer an anderen Knoten per E-Mail. Die Dauer der Aufzeichnung ist nur durch die verfügbare Speicherkapazität des Systems begrenzt.

Beenden der Konferenz

Die Konferenz endet zum geplanten Konferenzende oder vorzeitig wenn der Konferenzleiter sie beendet.

12.7.4 Permanente Konferenz

Eine permanente Konferenz ist zeitlich unbegrenzt. Die Konferenzteilnehmer können sich jederzeit einwählen.

Der Konferenzleiter speichert eine permanente Konferenz unter einem eigenen Namen. Sie bleibt bestehen bis er sie löscht.

Optionen beim Konfigurieren einer permanenten Konferenz

Der Initiator der Konferenz kann festlegen:

- Ob sich die Konferenzteilnehmer beim Eintreten in die Konferenz durch Eingabe von Konferenz-ID und Kennwort über die Telefontastatur authentifizieren müssen.

INFO: Mobility-Entry-Teilnehmer müssen vor ihrer Authentifizierung die Kennzahl für MFV-Nachwahl eingeben.

Das Standardkennwort für Konferenzen ist 123456. Der Konferenzleiter kann dies für Konferenzteilnehmer individuell ändern.

- In welcher Sprache die Ansagen zu Konferenzbeginn erfolgen sollen.

Starten der Konferenz

Sobald sich der erste Konferenzteilnehmer einwählt, öffnet das System bei allen internen Konferenzteilnehmern automatisch das Fenster mit dem virtuellen Konferenzraum, sofern der Konferenzteilnehmer myPortal for Desktop mit der klassischen Benutzeroberfläche oder myPortal for Outlook gestartet hat. Alle Konferenzteilnehmer wählen sich selbst ein. Das System kündigt jeden hinzukommenden Teilnehmer mittels Ansage an: "`... nimmt an der Konferenz teil.`"

Einwahl

Mittels Einwahlnummer kann sich jeder Konferenzteilnehmer jederzeit in die Konferenz einwählen. Bei Einwahl über einen ITSP muss dieser RFC 2833 (DTMF-Zeichen) unterstützen.

Aufzeichnen der Konferenz

Der Konferenzleiter kann die Konferenz automatisch oder manuell für sich und für alle verbundenen internen Konferenzteilnehmer aufzeichnen, sofern das Aufzeichnen von Gesprächen im System aktiviert ist. Teilnehmer des eigenen Knotens erhalten die Aufzeichnung in der Sprachbox, Teilnehmer an anderen Knoten per E-Mail. Die Dauer der Aufzeichnung ist nur durch die verfügbare Speicherkapazität des Systems begrenzt.

12.7.5 Offene Konferenz

Eine offene Konferenz ist für eine bestimmte Anzahl beliebiger Teilnehmer. Jeder Teilnehmer, der über die Zugangsdaten verfügt, kann sich einwählen.

Der Konferenzleiter speichert eine offene Konferenz unter einem eigenen Namen. Sie bleibt bestehen bis er sie löscht.

Optionen beim Konfigurieren einer offenen Konferenz

Der Initiator der Konferenz kann festlegen:

- Die Anzahl der Konferenzteilnehmer (max. 16).
- Ob sich die Konferenzteilnehmer beim Eintreten in die Konferenz durch Eingabe von Konferenz-ID und Kennwort über die Telefontastatur authentifizieren müssen.

INFO: Mobility-Entry-Teilnehmer müssen vor ihrer Authentifizierung die Kennzahl für MFV-Nachwahl eingeben.

Das Standardkennwort für Konferenzen ist 123456. Der Konferenzleiter kann dies für Konferenzteilnehmer individuell ändern.

- Welche gemeinsame Konferenz-ID für alle Konferenzteilnehmer gilt.
- In welcher Sprache die Ansagen zu Konferenzbeginn erfolgen sollen.

Starten der Konferenz

Alle Konferenzteilnehmer wählen sich selbst ein. Das System kündigt jeden hinzukommenden internen Teilnehmer mittels Ansage an: "`â€¦ nimmt an der Konferenz teil.`"

Einwahl

Mittels Einwahlnummer kann sich jeder Konferenzteilnehmer jederzeit in die Konferenz einwählen. Bei Einwahl über einen ITSP muss dieser RFC 2833 (DTMF-Zeichen) unterstützen.

Aufzeichnen der Konferenz

Der Konferenzleiter kann die Konferenz automatisch oder manuell für sich und für alle verbundenen internen Konferenzteilnehmer aufzeichnen, sofern das Aufzeichnen von Gesprächen im System aktiviert ist. Teilnehmer des eigenen Knotens erhalten die Aufzeichnung in der Sprachbox, Teilnehmer an anderen Knoten per E-Mail. Die Dauer der Aufzeichnung ist nur durch die verfügbare Speicherkapazität des Systems begrenzt.

12.7.6 Web Collaboration-Einbindung

Das System unterstützt mit myPortal for Desktop (Windows) und myPortal for Outlook bei Telefongesprächen, bei telefongesteuerten Telefonkonferenzen und bei applikationsgesteuerten Telefonkonferenzen die komfortable Einbindung des separaten Produktes Web Collaboration für die gleichzeitige multimediale Zusammenarbeit. Dies bietet Ihnen schnellen Zugriff auf Funktionen wie Desktop- und Anwendungsfreigabe, Dateifreigabe, Co-Browsing, Whiteboarding, URL-Push, IM-Chat und Video-Chat mit mehreren Teilnehmern.

Für die Einbindung der Web Collaboration muss dem Kommunikationssystem die Adresse des Web Collaboration Servers bekannt gegeben werden. Der Hersteller bietet den Web Collaboration Server im Internet als Dienst an (Public Server). Alternativ kann es sich hier auch um einen Server im Kundennetz oder bei einem Partner handeln (Custom Server). Befindet sich der Server im Kundennetz wird dieser vom Kommunikationssystem im Regelfall via http über den TCP-Port 5004 angesprochen. Bei der gehosteten Lösung im Internet (Public Server) wird hierfür eine gesicherte https-Verbindung verwendet, da über diese Verbindung Lizenznummer und Passwort übertragen werden. Standardmäßig wird dabei der TCP-Port 5100 verwendet.

> ***INFO:*** Für die Nutzung der Web Collaboration benötigt das Kommunikationssystem eine Internet-Verbindung (Default Router und DNS-Server). Verbindungen über Proxy werden nicht unterstützt.

Unterstützte Arten von Verbindungen

Die Web Collaboration-Einbindung unterstützt Telefongespräche sowie folgende Arten von applikationsgesteuerten Telefonkonferenzen des Systems:

- Ad-hoc-Konferenz
- geplante Konferenz
- permanente Konferenz

Eine Web Collaboration kann während eines Telefongesprächs (einer Konferenz) über das PopUp Fenster gestartet werden.

Beim Initiieren bzw. Konfigurieren einer Telefonkonferenz kann der Konferenzleiter eine Web Collaboration Sitzung zur gleichzeitigen Nutzung mit den selben Teilnehmern starten. Beim Verschieben bzw. Löschen oder Beenden einer Telefonkonferenz wird die zugehörige Web Collaboration Sitzung automatisch verschoben bzw. gelöscht.

Beim Start von Web Collaboration öffnet sich der Web Collaboration Client, dieser erfordert keine lokale Installation auf dem Desktop. Weitere Informationen finden Sie in der Web Collaboration Produktdokumentation.

> ***INFO:*** Damit Clients eine Web Collaboration automatisch starten können, muss beim Internetzugang der Clients über einen Proxy-Server die Proxy-Authentifizierung deaktiviert sein.

Verbinden mit der Web Collaboration Sitzung

Interne Konferenzteilnehmer mit UC PC-Clients werden beim Starten der Konferenz automatisch mit der entsprechenden Web Collaboration Sitzung verbunden. Hierfür wird FastViewer automatisch im Hintergrund heruntergeladen und geöffnet, was einige Sekunden dauern kann. Externe Konferenzteilnehmer mit bekannter E-Mail-Adresse erhalten per E-Mail einen entsprechenden Link für die Web Collaboration-Sitzung.

> ***INFO:*** Benutzer unter MAC OS müssen nach Beendigung einer Web Collaboration Sitzung den Hinweisdialog für die beendete Sitzung manuell schließen.

Bei einer geplanten Konferenz ist das Verbinden mit der Web Collaboration Sitzung bereits ab 5 Minuten vor dem geplanten Beginn der Konferenz möglich.

Konferenz-ID und Kennwort

Konferenz-ID und Kennwort für eine Web Collaboration-Sitzung sind jeweils indentisch mit Konferenz-ID und Kennwort der zugehörigen Telefonkonferenz.

Instant Messaging und Web Collaboration

Instant Messaging des Systems und Instant Messaging von Web Collaboration sind voneinander unabhängig: Sofortnachrichten aus einem UC-Client erscheinen nicht in einer Web Collaboration Sitzung des selben Teilnehmers und umgekehrt.

12.7.6.1 Wie Sie die Verbindung zum Web Collaboration Server (Custom Server) konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.
- Ein Internet-Zugang ist vorhanden.
- Für eine verschlüsselte Verbindung zum Web Collaboration Server (Custom Server) benötigen Sie eine Lizenznummer und ein Passwort.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Applikationen > Web Services**.

3) Navigieren Sie im Menübaum zu **Web Services > Web Collaboration**.

4) Aktivieren Sie das Optionsfeld **Custom Server**.

5) Wenn Sie eine verschlüsselte Verbindung zum Web Collaboration Server (Custom Server) aufbauen möchten, gehen Sie folgendermaßen vor:

a) Geben Sie in Feld **URL / IP-Adresse** die Adresse des Web Collaboration Servers (Custom Server) nach folgendem Muster ein:

`https://<URL Web Collaboration Server>:5100/xmlrpcsecure`

oder

`https://<IP-Adresse Web Collaboration Server>:5100/xmlrpcsecure`

b) Geben Sie im Feld **Lizenznummer** die Lizenznummer für die Verbindung zum Web Collaboration Server (Custom Server) ein.

c) Geben Sie in dem Feld **Passwort** das Passwort für die Verbindung zum Web Collaboration Server (Custom Server) ein.

6) Wenn Sie eine unverschlüsselte Verbindung zum Web Collaboration Server (Custom Server) aufbauen möchten, gehen Sie folgendermaßen vor:

a) Geben Sie in Feld **URL / IP-Adresse** die Adresse des Web Collaboration Servers (Custom Server) nach folgendem Muster ein:

```
http://<URL Web Collaboration Server>:5004/OscIn-
terface
```

oder

```
http://<IP-Adresse Web Collaboration Server>:5004/
OscInterface
```

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

12.7.6.2 Wie Sie die Verbindung zum Web Collaboration Server (Public Server) konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.
- Ein Internet-Zugang ist vorhanden.
- Für die verschlüsselte Verbindung zum Web Collaboration Server (Public Server) benötigen Sie eine Lizenznummer und ein Passwort.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Applikationen > Web Services**.

3) Navigieren Sie im Menübaum zu **Web Services > Web Collaboration**.

4) Aktivieren Sie das Optionsfeld **Public Server**.

5) Geben Sie im Feld **Lizenznummer** die Lizenznummer für die Verbindung zum Web Collaboration Server (Public Server) ein.

6) Geben Sie im Feld **Passwort** das Passwort für die Verbindung zum Web Collaboration Server (Public Server) ein.

INFO: Wenn Sie die Web Collaboration 5 min lang testen wollen, können Sie das Optionsfeld **Public Server (Demo Mode/Evaluation Mode)** aktivieren. Hierfür benötigen Sie keine Lizenznummer und kein Passwort.

---

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

12.7.6.3 Wie Sie die Verbindung zum Web Collaboration Server deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Applikationen > Web Services**.

3) Navigieren Sie im Menübaum zu **Web Services > Web Collaboration**.

4) Aktivieren Sie das Optionsfeld **Kein Web Collaboration Server**.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**. Die Option zum Starten einer Web Collaboration Sitzung ist in den UC Clients deaktiviert.

12.8 Sprach- und Faxnachrichten (UC Suite)

Die im System integrierten Dienste Sprach- und Faxnachrichten ermöglichen Teilnehmern über myPortal for Desktop und myPortal for Outlook das Empfangen und Verwalten von Sprach- und Faxnachrichten. Mit Fax Printer können Teilnehmer Faxnachrichten senden.

12.8.1 Sprachbox (UC Suite)

Die Sprachbox (UC Suite) zeichnet zentral Sprachnachrichten und mitgeschnittene Gespräche auf. Teilnehmer können darauf telefonisch sowie mit UC Smart Clients zugreifen.

Es werden nur Sprachnachrichten aufgezeichnet, die länger sind als zwei Sekunden.

Verwaltung von Sprachnachrichten

Als Teilnehmer können Sie Ihre Sprachnachrichten abhören:

- über PC mit myPortal for Desktop oder myPortal for Outlook
- über Ihr Telefon, wenn Ihr Anwesenheitsstatus **Büro** oder **CallMe** ist
- über ein beliebiges externes Telefon

Die Vermittlung kann über myAttendant auf Sprachnachrichten von Teilnehmern zugreifen, die dies zulassen.

Der Teilnehmer verwaltet die eingegangenen Sprachnachrichten mit den Ordnern, wie z. B. Posteingang, Abgespielt, Gespeichert oder Gelöscht.

Die Sprachnachrichten können auch zurückgespielt, angehalten und an einen anderen Teilnehmer weitergeleitet werden. Zusätzlich kann der Teilnehmer Sprachnachrichten im .wav-Format abspeichern und an eine beliebige E-Mail-Adresse weiterleiten.

Über die Sprachbox verwaltet der Teilnehmer auch aufgezeichnete Gespräche. Aufgezeichnete Gespräche werden in der Sprachbox mit einem entsprechenden Symbol gekennzeichnet.

INFO: Informationen zum Telefonmenü finden Sie in der Dokumentation UC Suite Telefon User Interface (TUI), Kurzbedienungsanleitung.

Absender einer Sprachnachricht zurückrufen

Beim Abhören einer Sprachnachricht kann der Teilnehmer direkt die Person zurückrufen, die ihm die Nachricht hinterlassen hat.

Als Administrator können Sie systemweit konfigurieren, ob Rückrufe aus der Sprachbox

- von jeder beliebigen Rufnummer ausgeführt werden können
- nur von eigenen Rufnummern des Teilnehmers ausgeführt werden können, welche in den Clients myPortal for Desktop, myPortal for Outlook, myAttendant bzw. myAgent unter Eigene persönliche Daten konfiguriert sind (**Nebenstelle**, **Mobilrufnummer**, **Externe Rufnummer 1**, **Externe Rufnummer 2**, **Private Rufnummer** und **Assistenten-Rufnummer**).

Aufbewahrungsdauer

Als Administrator können Sie die Aufbewahrungsdauer für Sprachnachrichten konfigurieren.

Priorisierung von Sprachnachrichten

Anrufer können Sprachnachrichten als normal, dringend oder vertraulich kennzeichnen.

In myPortal for Desktop und myPortal for Outlook wird die Priorisierung der vorliegenden Sprachnachrichten durch unterschiedliche Farben dargestellt.

Hört der Teilnehmer seine Sprachnachrichten über Telefon ab, dann erhält er als erstes die Information, wieviele Nachrichten dringend, vertraulich und normal sind. Dringenden Nachrichten werden zuerst wiedergegeben.

Werden die Sprachnachrichten als E-Mail weitergeleitet, werden als dringend gekennzeichnete Sprachnachrichten als E-Mail mit hoher Priorität gekennzeichnet.

Funktionsumfang der Sprachbox

Der Administrator kann den Funktionsumfang der Sprachbox festlegen. Er kann wählen zwischen:

- **Voll**
  Voller Funktionsumfang für die Sprachbox (Standardwert)
- **Kurzmenü**
- Nach der statusbezogenen oder persönlichen Ansage wird das Verbinden zum Empfang angeboten.
- **Kein Menü**
- Nach der Begrüßungsansage wird der Anrufer direkt zur Nachrichten-Aufzeichnung weitergeleitet.

Anzeigen neuer Nachrichten am Telefon

Neue Sprachnachrichten werden am Telefon signalisiert. Sobald die Sprachnachricht abgespielt wurde, werden die Anzeigen gelöscht.

Die Art der Signalisierung neuer Sprachnachrichten ist endgerätespezifisch:

- Bei allen Telefonen erfolgt eine akustische Signalisierung mittels Sonderwählton.
- Bei Systemtelefonen ohne Display leuchtet zusätzlich die Briefkasten-Taste (wenn eingerichtet).
- Bei Systemtelefonen mit Display leuchtet die Briefkasten-Taste (wenn eingerichtet) und im Display wird eine Meldung ausgegeben.

Benachrichtungsdienst

Über myPortal for Desktop oder myPortal for Outlook kann der Teilnehmer festlegen, ob die Information über das Eintreffen einer neuen Sprachnachricht weitergeleitet werden soll und zu welchem Ziel.

Der Teilnehmer kann bestimmen, ob die Nachricht als E-Mail weitergeleitet wird. Weiterhin kann der Teilnehmer bestimmen, ob er beim Eintreffen einer neuen Sprachnachricht durch einen Telefonanruf oder durch eine SMS benachrichtigt wird.

Sprache der Sprachbox

Als Administrator können Sie systemweit die standardmäßige Sprache der Sprachbox für das Menü und die systemeigenen Ansagen wählen.

Abhängigkeiten

Thema	Abhängigkeit
Nachricht über Telefon abspielen	Der Teilnehmer kann Sprachnachrichten über Telefon nur im Anwesenheitsstatus **Büro** oder **CallMe** abspielen. Bei allen anderen Einstellungen kann er die Nachricht nur über PC abspielen.

12.8.1.1 Wie Sie die Rufnummer der Sprachbox (UC Suite) konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Zentrale Telefonie**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Voicemail** zu starten.

4) Geben Sie die **VoiceMail Nummer** ein.

5) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

12.8.1.2 Wie Sie die Rufweiterschaltung zur Sprachbox (UC Suite) konfigurieren

Mit dem Wizard **Rufweiterschaltung** können Sie für einen Teilnehmer die Rufweiterschaltung zu seiner Sprachbox konfigurieren.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > User-Telefonie**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Rufweiterschaltung** zu starten. Es öffnet sich das Fenster **Anrufweiterschaltung konfigurieren**.

4) Wählen Sie im Bereich **Teilnehmer auswählen** den gewünschten Teilnehmer aus.

5) Ziehen Sie die **Sprachbox** mit der Maus und legen Sie sie im Fensterbereich **Rufweiterschaltung für Teilnehmer parametrieren** ab.

6) Ändern Sie ggf. die Zeit bis zur Rufweiterschaltung (Standard: 15 Sekunden).

7) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

12.8.1.3 Wie Sie Parameter der Sprachbox (UC Suite) konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen > OpenScape Business UC Suite**.
3) Klicken Sie auf **Server**.
4) Klicken Sie auf die **Sprachnachrichten**.
5) Wählen Sie in der Aufklappliste **VoiceMail-Sprache** die Sprache für die Menüsteuerung und die vordefinierten Ansagen Ihrer Sprachbox aus.
6) Legen Sie im Feld **Wiedergabereihenfolge für Sprachnachrichten** fest, in welcher Reihenfolge die Nachrichten abgespielt werden sollen.
7) Geben Sie im Feld **Aufzeichnungszeit Sprachnachricht** die Dauer in Sekunden ein.
8) Legen Sie im Feld **VoiceMail-Modus** den Umfang der Sprachbox fest.
9) Wenn Sie wollen, dass Rückrufe aus der Sprachbox nur an Rufnummern ausgeführt werden sollen, die in den UC Clients unter **Eigene persönliche Daten** eingetragen sind, aktivieren Sie das Kontrollkästchen **Rückruf von VM nur an bekannte Nummer zulassen**.
10) Klicken Sie auf **Speichern**.

12.8.1.4 Wie Sie die Aufbewahrungsdauer für Sprachnachrichten (UC Suite) konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen > OpenScape Business UC Suite**.
3) Klicken Sie auf **Server**.
4) Klicken Sie auf **Wartung**.
5) Geben Sie in den Feldern unter **Nachricht** jeweils die Aufbewahrungszeit in Tagen ein.
6) Klicken Sie auf **Speichern**.

12.8.1.5 Wie Sie eine Info für empfangene Sprachnachrichten (UC Suite) konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telephony Server > Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **System**.
4) Klicken Sie im Menübaum auf **Display**.
5) Aktivieren Sie im Bereich **Schalter** das Kontrollkästchen **Displaystatusanzeige bei Info-Meldung**.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

12.8.1.6 Wie Sie die Briefkastentaste für die Abfrage von Sprachnachrichten (UC Suite) konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards > Endgeräte/Teilnehmer**.
3) Klicken Sie auf **Bearbeiten** um den Wizard **Tastenprogrammierung** zu starten.
4) Wählen Sie den betreffenden Teilnehmer aus.
5) Wählen Sie in der erste Spalte die entsprechende Taste aus.
6) Wählen Sie in der Spalte **Tastenfunktionen** die Funktion **Briefkasten** aus.
7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

12.8.2 Ansagen der Sprachbox (UC Suite)

Ansagen der Sprachbox informieren Anrufer z. B. über den Anwesenheitsstatus eines Teilnehmers.

Standardansagen sind in allen Sprachen vorhanden. Als Teilnehmer können Sie persönliche Ansagen für die Sprachbox aufzeichnen oder importieren. Die entsprechende Standardansage wird dabei durch die persönliche Ansage

überschrieben. Als Administrator können Sie die Standardansagen durch den Import von Ansagen ändern. Persönliche Ansagen von Teilnehmern werden dabei überschrieben. Das System führt beim Importieren von Ansagen automatisch eine Pegelbegrenzung und Normalisierung durch, um die Anforderungen gemäß "USA / TIA 968 Signal Power Limitations" zu erfüllen.

> ***INFO:*** Stellen Sie vor der Benutzung von Ansagen bzw. Musik aus anderer Quelle sicher, dass Sie keine Copyright-Verletzung begehen.

Systemsprache Ansagen der Sprachbox

Die Systemsprache der Sprachbox wird bei der Länderinitialisierung eingestellt. Zusätzlich kann der Teilnehmer die Sprache seiner Sprachbox selbst einstellen. Ein Anrufer hört dann die teilnehmerbezogenen Ansagen in vom Teilnehmer eingestellten Sprache und die systembezogenen Ansagen in der Systemsprache.

Ansagen in Abhängigkeit von Anwesenheitsstatus und Profil

Abhängig vom Anwesenheitsstatus ändern sich automatisch die Ansagen der Sprachbox, z. B.: Ist der Anwesenheitsstatus **Besprechung**, dann lautet die Ansage z. B.: Der Teilnehmer ist in einer Besprechung bis heute 15.00 Uhr. Wenn das eingetragene Ende einer Besprechung erreicht ist, aber der Teilnehmer seinen Anwesenheitsstatus noch nicht auf Büro zurückgeändert hat, dann wird die Ansage der Sprachbox automatisch angepasst oder der Anwesenheitsstatus wechselt automatisch zurück auf Büro (durch den Teilnehmer konfigurierbar).

Die folgende Tabelle beschreibt, welche Begrüßung der Anrufer abhängig vom gesetzen Anwesenheitsstatus und dem eingestellten Profil hört. Das Anrufermenü bezieht sich auf den zentralen AutoAttendant. Das Profil bezieht sich auf den persönlichen AutoAttendant des Teilnehmers. Standardbegrüßung, Name und benutzerdefinierte Begrüßung für Profile sind vom Teilnehmer aufzuzeichnen. Abhängig von der Konfiguration kann das Anrufermenü unterschiedlich lang oder auch nicht verfügbar sein.

	Besetzt **Nicht angenommen** **Anrufschutz**	**Besprechung** **Krank** **Pause** **Außer Haus** **...**
Sprachbox mit Anwesenheitsstatus	Standardbegrüßung + Anrufermenü	Name + Anwesenheitsstatus + Anrufermenü

	Besetzt Nicht angenommen Anrufschutz	**Besprechung Krank Pause Außer Haus ...**
Sprachbox bei gesperrtem Anwesenheitsstatus	Standardbegrüßung + Anrufermenü (wenn aktiviert)	
Profile mit dynamischer Ansage	Benutzerdefinierte Begrüßung für Profil	Name + Anwesenheitsstatus + Benutzerdefinierte Begrüßung für Profil
Profile, wenn dynamische Ansage übersprungen werden soll	Benutzerdefinierte Begrüßung für Profil	

Hat ein Teilnehmer eingestellt, dass sein Präsenzstatus nicht an einen externen Anrufer übermitteln werden soll, bekommt der externe Anrufer bei jedem Anwesenheitsstatus außer "Büro" die "Besetzt"-Begrüßung, obwohl der angerufene Teilnehmer u.U. gar nicht besetzt ist. In diesem Fall sollte der Teilnehmer für die Begrüßung "Besetzt" eine Ansage definieren, dass er den Anruf nicht entgegennehmen kann.

12.8.2.1 Wie Sie eine Ansage für die Sprachbox (UC Suite) importieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.
- Einzuspielende Audiodateien liegen als PCM-Dateien mit folgenden Eigenschaften vor: 8 kHz, 16 bit, mono. Die Länge des Audio-Dateinamens beträgt maximal 30 Zeichen.

INFO: Sie können im Vorfeld mit Audio Wizard geeignete Audiodateien erstellen und dabei zwei Quellen abmischen, z. B. Hintergrundmusik und Ansage.

INFO: Stellen Sie vor der Benutzung sicher, dass Sie keine Copyright-Verletzung begehen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Datei-Upload** zu starten.

4) Wählen Sie in der Registerkarte **Audiodatei-Manager** als **Upload-Ziel** den Eintrag **VoiceMail-Begrüßung** aus.

5) Wenn Sie eine Audio-Datei einspielen wollen, gehen Sie folgendermaßen vor:

   a) Klicken Sie auf **Durchsuchen**, um eine entsprechende Audio-Datei auszuwählen.

   b) Im Bereich **Details Audiodatei** sehen Sie die Eigenschaften der Audio-Datei, wie Dateiname, Dateigröße, Bitrate usw.

   c) Klicken Sie auf **Upload**.

6) Wenn Sie eine Ansage über ein Telefon aufnehmen wollen, gehen Sie folgendermaßen vor:

   a) Wählen Sie unter **Nebenstelle** das Telefon aus, mit dem die Ansage aufgenommen werden soll.

   b) Klicken Sie auf **Anrufen**. Das ausgewählte Telefon klingelt.

   c) Heben Sie den Telefonhörer ab und klicken Sie auf **Aufzeichnen**.

   d) Sprechen Sie Ihre Ansage in den Telefonhörer und klicken Sie abschließend auf **Beenden**.

   e) Mit **Wiedergeben** können Sie sich Ihre Aufzeichnung nochmals anhören.

12.8.2.2 Wie Sie die Sprache für Ansagen der Sprachbox (UC Suite) ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Applikationen > OpenScape Business UC Suite**.

3) Klicken Sie auf **Server**.

4) Klicken Sie auf **Sprachnachrichten**.

5) Wählen Sie die **VoiceMail-Sprache** aus der Aufklappliste aus.

6) Klicken Sie auf **Speichern**.

12.8.3 Faxbox

Die Faxbox ermöglicht Teilnehmern das Empfangen und Verwalten von Faxnachrichten ohne Faxgerät über myPortal for Desktop oder myPortal for Outlook.

Als Administrator können Sie für lizenzierte Teilnehmer eine Faxbox konfigurieren. Außerdem können Sie Faxgeräte oder Faxserver über die a/b- bzw. ISDN-Schnittstelle anschließen.

Über myPortal for Desktop oder myPortal for Outlook können Sie als Teilnehmer auf Ihre Faxnachrichten zugreifen. myAttendant kann auf die Faxnachrichten der Teilnehmer zugreifen, die dies zulassen.

Verwaltung von Faxnachrichten

Der Teilnehmer kann die empfangenen Faxnachrichten verwalten, indem er sie in die Ordner, wie z. B. Gespeichert oder Gelöscht, verschiebt. Die Faxnachrichten können auch an einen anderen Teilnehmer weitergeleitet werden. Zusätzlich kann der Teilnehmer Faxnachrichten als PDF- oder TIFF-Datei speichern und an eine beliebige E-Mail-Adresse weiterleiten.

Der Administrator kann systemweit einrichten, ob die Faxnachricht als TIFF-Datei (Standard) oder als PDF-Datei gespeichert werden soll.

Aufbewahrungsdauer für Faxnachrichten

Das System löscht automatisch Faxnachrichten, deren Alter folgende Aufbewahrungsdauer überschreitet:

Faxnachricht	Aufbewahrungsdauer (Tage)
neu	120
gelesen	365
gesendet	365
gelöscht	60

12.8.3.1 Wie Sie eine Faxbox für Teilnehmer hinzufügen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Endgeräte/Teilnehmer**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **IP-Endgeräte** zu starten.

4) Klicken Sie in das Feld **Fax Rufnr** des Teilnehmers und geben Sie die Fax-Rufnummer ein, unter welcher der Teilnehmer Faxnachrichten empfangen kann (der vorbelegte Bindestrich muss gelöscht werden).

5) Wenn für die Faxbox eine Durchwahlnummer konfiguriert werden soll, klicken Sie in das Feld **Fax Durchwahl** und geben die Fax-Durchwahlnummer ein (der vorbelegte Bindestrich muss gelöscht werden).

6) Klicken Sie auf **OK & Weiter**. Bei Bedarf können Sie sich über **Drucken** eine Teilnehmerliste mit den konfigurierten Fax-Rufnummern ausdrucken lassen.

7) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**, um den Wizard abzuschließen.

12.8.3.2 Wie Sie den Dateityp für gespeicherte Faxnachrichten (UC Suite) konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Applikationen > OpenScape Business UC Suite**.

3) Klicken Sie auf **Server**.

4) Klicken Sie auf **Allgemeine Einstellungen**.

5) Wenn Sie möchten, das Faxnachrichten als PDF-Dateien abgespeichert werden können, dann aktivieren Sie im Bereich **Faxformat** das Kontrollkästchen **Als Faxformat PDF verwenden**.

6) Wenn Sie möchten, das Faxnachrichten als TIFF-Dateien abgespeichert werden können, dann deaktivieren Sie im Bereich **Faxformat** das Kontrollkästchen **Als Faxformat PDF verwenden**.

7) Klicken Sie auf **Speichern**.

12.8.4 Senden von Faxnachrichten mit Fax Printer

Fax Printer ist eine Anwendung für den Versand von Faxnachrichten aus Windows-Anwendungen wie z. B. Microsoft Word mit zentral bereitgestellten oder individuell erstellten Deckblättern.

Fax Printer besteht aus folgenden Komponenten:

- Fax Printer Cover Editor
- Fax Printer Driver

Fax Printer kann mit allen gängigen Windows-Programmen verwendet werden. Fax-Gruppen erleichtern die Verteilung. Faxnachrichten werden als E-Mail oder direkt auf den Desktop gesendet. Ein Popup-Fenster informiert den Teilnehmer über den Erfolg des Versands.

Kopfzeilen

Als Administrator können Sie verschiedene Kopfzeilen für die Benutzer von Fax Printer konfigurieren. Sie können eine Kopfzeile als Standard festlegen. Kopfzeilen können folgende Elemente enthalten:

Detail	Platzhalter
Datum / Uhrzeit	{{date_time}}
Firmenname	{{company_name}}
Benutzername	{{user_name}}
Firmen-Rufnr.	{{company_number}}
Seitenzahl	{{page_number}}
Anzahl der Seiten	{{page_count}}

Kopfzeilen von Faxnachrichten, die mit Fax Printer gesendet werden, dürfen keine Sonderzeichen oder Umlaute enthalten, sondern nur Zeichen des ANSI-Zeichensatzes. Da die Kopfzeile grundsätzlich den Namen des Absenders enthalten kann, dürfen die Namen der Teilnehmer keine Sonderzeichen oder Umlaute enthalten.

12.8.4.1 Wie Sie ein zentrales Faxdeckblatt hinzufügen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.
- Ein Fax-Deckblatt liegt als .ocp-Datei vor.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Datei-Upload** zu starten.

4) Klicken Sie auf die Registerkarte **Upload des zentralen Fax-Deckblatts**.

5) Klicken Sie auf **Durchsuchen**.

6) Wählen Sie eine .ocp-Datei aus.

7) Klicken Sie auf **Öffnen**.

8) Geben Sie in **Dateiname** einen Namen für das Faxdeckblatt ein.

9) Geben Sie eine **Beschreibung** für das Faxdeckblatt ein.

10) Klicken Sie auf **Upload**.

11) Klicken Sie nach beendetem Upload auf **OK**.

12) Wenn Sie dieses Faxdeckblatt als Standard setzen möchten, klicken Sie in der Liste der Faxdeckblätter auf dieses Faxdeckblatt und anschließend auf **Als Standard setzen**.

13) Klicken Sie auf **Speichern**.

12.8.4.2 Wie Sie das zentrale Faxdeckblatt bearbeiten

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.
3) Klicken Sie auf **Bearbeiten** um den Wizard **Datei-Upload** zu starten.
4) Klicken Sie auf die Registerkarte **Upload des zentralen Fax-Deckblatts**.
5) Klicken Sie in der Liste der Faxdeckblätter auf das entsprechende Faxdeckblatt.
6) Klicken Sie auf **Bearbeiten**.
7) Geben Sie in **Dateiname** einen Namen für das Faxdeckblatt ein.
8) Geben Sie eine **Beschreibung** für das Faxdeckblatt ein.
9) Klicken Sie auf **Speichern**.

12.8.4.3 Wie Sie eine Kopfzeile für Fax Printer hinzufügen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.
3) Klicken Sie auf **Bearbeiten** um den Wizard **Faxkopfzeilen** zu starten.
4) Klicken Sie auf **Hinzufügen**.
5) Geben Sie **Name** für die Faxkopfzeile ein.
6) Um Details zur Kopfzeile hinzuzufügen, klicken Sie in der gewünschten Reihenfolge auf die entsprechende Schaltflächen **Datum / Uhrzeit**, **Firmenname**, **Benutzername**, **Firmen-Rufnr.**, **Seitenzahl** und **Anzahl der Seiten**. Für jedes Detail erscheint ein entsprechender Platzhalter im Feld **Text**.
7) Um ein Detail aus der Kopfzeile zu entfernen, markieren Sie in Feld **Text** den entsprechenden Platzhalter, z. B. `{{page_count}}` (**Anzahl der Seiten**) und drücken Sie die Taste `Entf`.
8) Geben Sie bei Bedarf in Feld **Text** zusätzlichen Text ein, z. B. " von " zwischen den Platzhaltern `{{page_number}}` (**Seitenzahl**) und `{{page_count}}` (**Anzahl der Seiten**).

9) Klicken Sie auf **Speichern**.

12.8.4.4 Wie Sie eine Kopfzeile für Fax Printer ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Applikationen > UC Suite**.

3) Klicken Sie auf **Faxkopfzeilen**.

4) Klicken Sie in der Liste der Faxkopfzeilen auf die gewünschte Faxkopfzeile.

5) Klicken Sie auf **Bearbeiten**.

6) Geben Sie **Name** für die Faxkopfzeile ein.

7) Um Details zur Kopfzeile hinzuzufügen, klicken Sie in der gewünschten Reihenfolge auf die entsprechende Schaltflächen **Datum / Uhrzeit**, **Firmenname**, **Benutzername**, **Firmen-Rufnr.**, **Seitenzahl** und **Anzahl der Seiten**. Für jedes Detail erscheint ein entsprechender Platzhalter im Feld **Text**.

8) Um ein Detail aus der Kopfzeile zu entfernen, markieren Sie in Feld **Text** den entsprechenden Platzhalter, z. B. `{{page_count}}` (**Anzahl der Seiten**) und drücken Sie die Taste `Entf`.

9) Geben Sie bei Bedarf in Feld **Text** zusätzlichen Text ein, z. B. " von " zwischen den Platzhaltern `{{page_number}}` (**Seitenzahl**) und `{{page_count}}` (**Anzahl der Seiten**).

10) Klicken Sie auf **Speichern**.

12.8.4.5 Wie Sie eine Kopfzeile für Fax Printer löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Faxkopfzeilen** zu starten.

4) Klicken Sie in der Liste der Faxkopfzeilen auf die gewünschte Faxkopfzeile.

5) Klicken Sie auf **Entfernen**.

12.8.5 Benachrichtigungsdienst für neue Nachrichten (UC Suite)

Das System kann Sie als Teilnehmer über eine neue Nachricht auf Wunsch per E-Mail, telefonisch oder per SMS informieren.

Der Benachrichtigungsdienst arbeitet folgendermaßen:

Benachrich-tigung	für Sprachnachricht	für Faxnachricht	Voraussetzung
E-Mail	Sie erhalten eine E-Mail mit der Nachricht als angehängte WAV-Datei, Datum und Uhrzeit des Empfangs, Dauer der Nachricht und sofern verfügbar Rufnummer sowie Name des Absenders. Falls die Größe der WAV-Datei 10 MB überschreitet, wird sie nicht an die E-Mail angehängt. Sprachnachrichten mit Priorität "Dringend" werden als E-Mail mit Wichtigkeit "Hoch" zugestellt. E-Mails mit einer Sprachnachricht haben in Outlook ein eigenes Symbol. Falls Sie ein IMAP-Postfach verwenden, welches nur die E-Mail-Header anzeigt, erscheint stattdessen das für E-Mails übliche Symbol.	Sie erhalten eine E-Mail mit der Nachricht als angehängte PDF- oder TIFF-Datei, Datum und Uhrzeit des Empfangs, Anzahl der Seiten und sofern verfügbar Rufnummer sowie Name des Absenders. Falls die Größe der PDF- oder TIFF-Datei 10 MB überschreitet, wird sie nicht an die E-Mail angehängt. E-Mails mit einer Faxnachricht haben in Outlook ein eigenes Symbol. Falls Sie ein IMAP-Postfach verwenden, welches nur die E-Mail-Header anzeigt, erscheint stattdessen das für E-Mails übliche Symbol.	E-Mail-Versand ist im System konfiguriert. Die entsprechende Adresse wird als Absender verwendet.
SMS	Sie erhalten eine SMS an die von Ihnen festgelegte Rufnummer über den Eingang der Nachricht		SMS-Template ist konfiguriert
telefonisch	Ihre Sprachbox ruft Sie unter der von Ihnen festgelegten Rufnummer an und spielt die Nachricht ab.	-	

Sie können als Teilnehmer jede Art der Benachrichtigung für jeden Anwesenheitsstatus separat aktivieren oder deaktivieren. Die telefonische Benachrichtigung können Sie auf die vom Administrator konfigurierten Geschäftszeiten einschränken. Sie können Anzahl und Intervalle für wiederholte Versuche der telefonischen Benachrichtigung festlegen.

12.8.6 E-Mail-Versand

E-Mail-Versand ermöglicht die Benachrichtigung von Teilnehmern bei neuen Sprach- und Faxnachrichten sowie des Administrators bei Systemmeldungen.

12.8.6.1 Wie Sie den E-Mail-Versand konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.
- Es ist ein E-Mail-Konto mit einem Kennwort bei einem E-Mail-Provider vorhanden und Sie kennen die Zugangsdaten.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Service-Center > E-Mail-Weiterleitung**.

3) Geben Sie den **Postausgangs-Server (SMTP)** für den E-Mail-Server ein, der für den E-Mail-Versand genutzt werden soll, z. B. `smtp.web.de`. Erfragen Sie den Postausgangs-Server ggf. bei Ihrem E-Mail-Provider.

> ***INFO:*** In einigen Fällen funktioniert der E-Mail-Versand nicht, weil der Name des Postausgangs-Servers nicht aufgelöst werden kann. Zur Behebung des Problems müssen Sie anstelle des Namens die IP-Adresse des Servers eingeben.

4) Wenn eine sichere Verbindung erforderlich ist, aktivieren Sie das Kontrollkästchen. Erfragen Sie ggf. bei Ihrem E-Mail-Provider, ob diese Option aktiviert werden muss.

5) Geben Sie den **Benutzernamen** des E-Mail-Kontos ein.

6) Geben Sie unter **Kennwort** und **Kennwort wiederholen** das Kennwort des E-Mail-Kontos ein.

7) Geben Sie die **E-Mail-Adresse** ein, z. B. `max.mustermann@web.de`.

8) Wenn Sie den E-Mail-Versand nun testen möchten, gehen Sie folgendermaßen vor:

a) Klicken Sie auf **Weiterleitung testen**.

b) Geben Sie unter **Senden an E-Mail-Adresse** die E-Mail-Adresse eines E-Mail-Postfachs ein, auf das Sie Zugriff haben.

c) Geben Sie **Betreff in der Email**.

d) Klicken Sie auf **Testmail senden**.

e) Prüfen Sie, ob Sie die E-Mail erhalten haben.

f) Wenn der E-Mail-Versand nicht erfolgreich war, klicken Sie auf **Zurück** und korrigieren Sie Ihre E-Mail-Einstellungen (ab Schritt 3).

9) Klicken Sie auf **OK und Weiter** und anschließend auf **Beenden**.

12.8.7 SMS-Template

Ein SMS-Template ermöglicht die SMS-Benachrichtigung von Teilnehmern bei neuen Sprachnachrichten.

Zum Empfang von SMS-Benachrichtigungen muss zunächst eine persönliche mobile E-Mail-Adresse des jeweiligen Providers aktiviert werden. Der Teilnehmer sendet dazu eine Aktivierungs-SMS an eine Kurzwahl-Nummer. Der Teilnehmer erhält dann per SMS seine persönliche E-Mail-Adresse, die sich in der Regel aus der Rufnummer und dem Gateway-Namen zusammensetzt. So wäre z. B. für einen T-Mobile-Kunden mit der Rufnummer 0171/1234 567 die mobile E-Mail-Adresse: 01711234567@t-mobile-sms.de. Analog gilt dies auch für andere Netze.

Ein SMS-Template besteht aus den Bereichen Template-Details und SMS-Details. Der Administrator muss im Bereich Template-Details den Namen des Templates eingeben, der üblicherweise der Name des E-Mail-to-SMS-Providers ist.

Die Angaben im Bereich SMS-Details sind abhängig vom Provider. Bei Empfänger muss der Administrator die E-Mail-Adresse eingeben, an welche die SMS geschickt werden soll. Die Angaben in der Betreffzeile sind entweder frei wählbar oder der Administrator muss hier z. B. die Kundennummer eintragen.

> ***INFO:*** Jeder Provider benötigt ein spezifisches Template. Die erforderlichen Daten erfahren Sie beim jeweiligen Mobilfunk-Provider.

Platzhalter

SMS-Templates können in Feld **Empfänger**, **Betreff** oder **Text** folgende Platzhalter enthalten:

Detail	Platzhalter
Die Mobilfunknummer, an die gesendet werden soll	`{{MobileNumber}}`
Name oder Rufnr. des Absenders	`{{Sender}}`
Datum und Uhrzeit des Nachrichteneingangs	`{{DateTime}}`
Rufnummer des Anrufers	`{{CallingNumber}}`
Priorität der Nachricht	`{{Priority}}`

Systemspezifische Informationen

Die Länge der Nachricht wird auf die ersten 160 Zeichen reduziert.

12.8.7.1 Wie Sie ein SMS-Template hinzufügen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Templates** zu starten.

4) Klicken Sie auf **Erstellen**.

5) Geben Sie **Template-Name** ein.

6) Geben Sie **Name des Autors** ein.

7) Wenn Sie einen Platzhalter einfügen möchten, führen Sie folgende Schritte durch:

a) Klicken Sie in das Feld, in dem Sie den Platzhalter einfügen möchten: **Empfänger**, **Betreff** oder **Text**.

b) Wählen Sie in der Aufklappliste **VSL-Felder** den gewünschten Platzhalter.

c) Klicken Sie auf **Einfügen**.

d) Wenn Sie weitere Platzhalter einfügen möchten, wiederholen Sie Schritt 7 a-c entsprechend.

8) Geben Sie den **Empfänger** ein.

9) Geben Sie den **Betreff** ein.

10) Geben Sie den **Text** ein.

11) Klicken Sie auf **Erstellen**.

12.8.7.2 Wie Sie ein SMS-Template bearbeiten

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Templates** zu starten.

4) Wählen Sie in der Aufklappliste **SMS-Templates** das gewünschte SMS-Template.

5) Klicken Sie auf **Bearbeiten**.

6) Geben Sie **Template-Name** ein.

7) Geben Sie **Name des Autors** ein.

8) Wenn Sie einen Platzhalter einfügen möchten, führen Sie folgende Schritte durch:

a) Klicken Sie in das Feld, in dem Sie den Platzhalter einfügen möchten: **Empfänger**, **Betreff** oder **Text**.

b) Wählen Sie in der Aufklappliste **VSL-Felder** den gewünschten Platzhalter.

c) Klicken Sie auf **Einfügen**.

d) Wenn Sie weitere Platzhalter einfügen möchten, wiederholen Sie Schritt 8 a-c entsprechend.

9) Geben Sie den **Empfänger** ein.

10) Geben Sie den **Betreff** ein.

11) Geben Sie den **Text** ein.

12) Klicken Sie auf **Erstellen**.

12.8.7.3 Wie Sie ein SMS-Template entfernen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Templates** zu starten.

4) Wählen Sie in der Aufklappliste **SMS-Templates** das gewünschte SMS-Template.

5) Klicken Sie auf **Entfernen**.

12.8.8 Fax over IP (T.38-Fax)

Fax over IP ermöglicht die Übertragung von Faxnachrichten nach Standard G2 und G3 über das Internet mittels Netzwerkprotokoll IFP (Internet Facsimile Protocol).

UC Suite kann generell bis zu 8 gleichzeitige Faxverbindungen verarbeiten. OpenScape Busines X3/X5/X8 als ISDN-Gateway kann abhängig vom DSP-Modul 3 bis 12 gleichzeitige Faxe verarbeiten. Beide Parameter bestimmen die Anzahl gleichzeitiger T.38-Faxverbindungen.

Das System unterstützt für T.38 folgende Szenarien:

- Ein Teilnehmer erhält Faxnachrichten über einen ITSP (Internet Telefonie Service Provider) an seine Faxbox und versendet mit Fax Printer über den ITSP nach extern.
- Ein Teilnehmer erhält Faxnachrichten über Mediatrix 4102S (SIP) an seine Faxbox und versendet mit Fax Printer über Mediatrix 4102S (SIP).
- Ein Teilnehmer erhält Faxnachrichten über einen ITSP (Internet Telefonie Service Provider) auf ein Faxgerät, das direkt an einer analogen oder ISDN-Schnittstelle angeschlossen ist und versendet von diesem Faxgerät über den ITSP nach extern.
- Ein Teilnehmer erhält Faxnachrichten über einen ITSP auf ein Faxgerät, das an Mediatrix 4102S angeschaltet ist und versendet von diesem Faxgerät über Mediatrix 4102S und ITSP nach extern.
- Ein Teilnehmer erhält Faxnachrichten über ISDN auf ein Faxgerät, das an Mediatrix 4102S angeschaltet ist und versendet von diesem Faxgerät über Mediatrix 4102S und ISDN nach extern.
- Ein Teilnehmer versendet Faxnachrichten von einem Faxgerät, das an Mediatrix 4102S angeschaltet ist auf ein anderes Faxgerät, das auch an Mediatrix 4102S angeschaltet ist.
- Interne Faxnachricht von einem Faxgerät an einer ISDN-Schnittstelle an ein Faxgerät an Mediatrix 4102S und umgekehrt.
- Interne Faxnachricht von einem Faxgerät an einer ISDN-Schnittstelle auf eine Faxbox und umgekehrt.

INFO: Für die Faxbox ist im System T.38 zu aktivieren. Bei Faxversand vom Kommunikationssystem über einen ITSP muss dieser T.38 unterstützen.

12.8.8.1 Wie Sie Fax over IP (T.38-Fax) aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telephony Server > Sprachgateway**.

3) Klicken Sie im Menübaum auf **Sprachgateway**.

4) Klicken Sie im Menübaum auf **Codec-Parameter**.

5) Wählen Sie im Bereich **T.38-Fax** eine der folgenden Möglichkeiten:

- Wenn Sie Fax over IP (T.38-Fax) aktivieren möchten, aktivieren Sie das Kontrollkästchen **T.38-Fax**.

- Wenn Sie Fax over IP (T.38-Fax) deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **T.38-Fax**.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

12.9 Instant Messaging (UC Suite)

Instant Messaging ist die Kommunikation mittels Sofortnachrichten (Chat).

12.9.1 Sofortnachrichten (UC Suite)

Mittels Sofortnachrichten können Sie mit anderen Kommunikationspartnern chatten. Das System unterstützt sowohl Benutzer von UC Smart als auch einen externen Kommunikationspartner via XMPP und Multi-User-Chat sowie beides in Kombination.

Sofortnachrichten sind mit folgenden Clients möglich:

- myPortal for Desktop
- myPortal for Outlook
- myAgent
- myAttendant

Als Administrator können Sie Sofortnachrichten systemweit aktivieren oder deaktivieren. Gesendete und empfangene Sofortnachrichten werden bei den Kommunikationspartnern als Dialog angezeigt. Beim Auswählen eines Empfängers zeigt der Client an, ob der Kommunikationspartner momentan online ist. Falls ein Kommunikationspartner offline ist, geschieht mit der Sofortnachricht abhängig von der Art des ausgewählten Empfängers Folgendes:

Empfänger	Verhalten
Einzelne Teilnehmer	Die Sofortnachricht wird bei der nächsten Anmeldung angezeigt.
Gruppe in Favoriten	Die Sofortnachricht wird bei jenen Teilnehmern die offline sind nie angezeigt.

Externe Sofortnachrichten

Als Teilnehmer können Sie mit *einem* externen XMPP-Kommunikationspartner (z. B. Benutzer von Google Talk) chatten.

Multi-User Chat

Multi-User Chat ist der Austausch von Sofortnachrichten mit mehreren Kommunikationspartnern. Dabei unterstützt das System auch maximal einen externen XMPP-Kommunikationspartner.

Instant Messaging und Web Collaboration

Instant Messaging des Systems und Instant Messaging von Web Collaboration sind voneinander unabhängig: Sofortnachrichten aus einem UC Client erscheinen nicht in einer Web Collaboration Sitzung des selben Teilnehmers und umgekehrt.

12.9.1.1 Wie Sie Sofortnachrichten (UC Suite) aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Applikationen > OpenScape Business UC Suite**.

3) Klicken Sie auf **Server**.

4) Klicken Sie auf **Allgemeine Einstellungen**.

5) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie Sofortnachrichten systemweit aktivieren möchten, deaktivieren Sie das Kontrollkästchen **Sofortnachricht versenden deaktivieren**.
- Wenn Sie Sofortnachrichten systemweit deaktivieren möchten, aktivieren Sie das Kontrollkästchen **Sofortnachricht versenden deaktivieren**.

INFO: Die Deaktivierung von Sofortnachrichten ist nicht wirksam für aktuell bestehende Sofortnachrichten-Fenster.

6) Klicken Sie auf **Speichern**.

12.10 AutoAttendant

AutoAttendant gibt Anrufern abhängig vom Anwesenheitsstatus des gerufenen Teilnehmers Auswahlmöglichkeiten für die Weiterleitung von Sprachanrufen zu festgelegten Rufnummern oder zu dessen Sprachbox. Anrufer treffen ihre Auswahl durch Eingabe von Ziffern am Telefon.

12.10.1 Persönlicher AutoAttendant

Der persönliche AutoAttendant ist der vom Teilnehmer konfigurierbare AutoAttendant.

Persönlicher AutoAttendant

Als Teilnehmer können Sie für Ihre Rufnummer mit myPortal for Desktop oder mit myPortal for Outlook:

- Ansagen für den persönlichen AutoAttendant aufzeichnen oder importieren
- Profile für den persönlichen AutoAttendant konfigurieren

Entsprechende Anrufe werden zuerst vom zentralen AutoAttendant behandelt.

13 Funktionen am Telefon

Das Kommunikationssystem bietet vielfältige Telefonie-Leistungsmerkmale, angefangen bei z. B. Halten, Makeln und Rückfrage, über unterschiedliche Anrufsignalisierungen bis hin zu Rufweiterschaltung und Anrufumleitung.

13.1 Anrufen

>Das Kommunikationssystem bietet verschiedene Möglichkeiten Anrufe zu tätigen, unter anderem Direktruf oder Kurzwahl.

13.1.1 Ziffernwahl

Bei der Ziffernwahl wird die Wahl jeder Ziffer direkt nach der Eingabe ausgesendet.

Der Verbindungsaufbau beginnt sofort bei Eingabe der ersten Ziffer. Der Teilnehmer hat dadurch keine Möglichkeit zum Editieren der Wahl.

13.1.2 Blockwahl

Bei der Blockwahl wird die Verbindung aufgebaut, wenn die vollständige Rufnummer eingegeben wurde. Die Rufnummer wird in einem einzigen Block übertragen.

Die Aussendung der Wahl kann durch Eingabe des Wahlendekennzeichens # gestartet werden.

Blockwahl ist zwingend vorgeschrieben für:

- ITSP-Amtsanschluss
- ISDN-Primärmultiplexanschluss in USA

Nach Ablauf von 5 Sekunden ohne Zifferneingabe, wird die zuletzt eingegebene Ziffer als letzte Ziffer des Rufnummernblocks interpretiert.

13.1.3 Keypad-Wahl

In verschiedenen Ländern werden Dienste digitaler Amtsanschlüsse über Keypad-Wahl und nicht funktional gesteuert. Um diese Dienste im PSTN zu aktivieren, kann die sogenannte Stimulus-Schnittstelle genutzt werden.

Das Leistungsmerkmal ist in Manager E zu konfigurieren.

Beim Teilnehmer erfolgt die Quittierung des Meldungsverkehrs über Displayanzeigen. Dementsprechend kann Keypad-Wahl ausschließlich über Telefone mit Display (optiPoint, -OpenStage), Mobiltelefone (Cordless) mit optiPoint-Menüführung und IP-Telefone mit Stimulus-Schnittstelle erfolgen. ISDN-Telefone werden nicht unterstützt. Der jeweilige Netzprovider bestimmt, welche Dienste über Keypad-Wahl genutzt werden können.

Ein berechtigter Teilnehmer kann Keypad-Wahl über das Servicemenü oder über die Kennzahl *503 aktivieren. Dies ist ausschließlich aus dem Ruhezustand möglich. Anschließend muss eine ISDN-Amtsleitung gewählt werden, über die das Leistungsmerkmal ablaufen soll.

In Abhängigkeit von den vom Amt gesendeten Meldungen (z. B. bei Connect) kann Keypad-Wahl Einträge in die Gesprächsdatenerfassung zur Folge haben. Protokolliert werden die Rufnummer des ausführenden Teilnehmers, die verwendete Leitung und der Zeitraum der Nutzung des Leistungsmerkmals.

INFO: Über Keypad-Wahl ausgeführte Aktionen unterliegen keiner Kontrolle durch das System. Missbräuchliche Nutzung, wie z. B. Gebührenmissbrauch oder Amtsleitungsblockierung, kann durch das System nicht verhindert werden.

Der Kunde ist darüber zu informieren, dass er selbst für Schäden haftet, welche durch Missbrauch dieses Leistungsmerkmals entstehen.

13.1.4 Wahlendeerkennung

Das Wahlende wird entweder automatisch nach 5 Sekunden erkannt oder manuell vom Benutzer durch das Wahlendekennzeichen "#" angezeigt.

13.1.5 Editieren der Wahl

Mit Editieren der Wahl kann der Teilnehmer die eingegebenen Ziffern der Rufnummer verändern. Diese Funktion ist bei Mobiltelefonen üblich. Eine Rufnummer kann nur während der Eingabe korrigiert werden.

Eine eingegebene Ziffernfolge kann von rechts nach links, durch Tastendruck jeweils um eine Ziffer gelöscht werden. Nach vollständiger Eingabe der korrekten Ziffernfolge kann die Wahlaussendung über die Bestätigen-Taste oder durch Abheben des Hörers erfolgen.

Das Editieren einer gespeicherten Rufnummer, z. B. für die Wahlwiederholung, ist nicht möglich.

INFO: Editieren der Wahl ist für jeden Teilnehmer einzeln aktivierbar.

Abhängigkeiten

Thema	Abhängigkeit
Anklopfen	Anklopfen während des Editierens ist möglich, da sich das Telefon im Wahlaufnahmezustand befindet und damit für kommenden Verkehr belegt ist.
Rückfrage	Nach einer Rückfrage befindet sich das Telefon im Wahlaufnahmezustand. Das Editieren von Rufnummerziffern ist damit möglich.

13.1.5.1 Wie Sie das Editieren der Wahl aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Teilnehmer**.

3) Klicken Sie im Menübaum auf **Teilnehmer**.

4) Klicken Sie im Menübaum auf den Teilnehmer (Index - Rufnummer - Name).

5) Klicken Sie auf die Registerkarte **Teilnehmer-Flags ändern**.

6) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie die Funktion aktivieren möchten, aktivieren Sie das Kontrollkästchen **Editieren der Wahl**.
- Wenn Sie die Funktion deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Editieren der Wahl**.

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

13.1.6 Wahlwiederholung

Bei jedem externen Gesprächsaufbau erfolgt eine Speicherung der gewählten Rufnummer. Ist das Ziel besetzt oder nicht erreichbar, kann der Teilnehmer die anschließend Wahlwiederholung nutzen um dieselbe Nummer erneut zu wählen.

Kurzwahlnummern werden ebenfalls in den Wahlwiederholungsspeicher geschrieben.

Die Wahl interner Rufnunmmern berührt den Wahlwiederholungsspeicher nicht.

Eventuelle Nachwahlziffern (auch MFV-Zeichen genannt) werden nicht als Wahlinformation angesehen und daher nicht abgespeichert (z. B. Ziffern, die an eine angeschlossene Sprachbox gesendet werden).

Die Funktion Wahlwiederholung kann nur über die Taste erfolgen, nicht über einen Zugangscode.

Durch Betätigen der Wahlwiederholungstaste können diese Rufnummern gezielt aufgerufen und erneut für einen Gesprächsaufbau verwendet werden. Bei einmaligem Tastendruck erfolgt die Wahl der zuletzt gewählten Rufnummer. Bei zweifachem Tastendruck erfolgt die Wahl der vorletzten Rufnummer. Bei dreifachem Tastendruck erfolgt die Wahl der am ältesten gespeicherten Rufnummer.

Nach Drücken der Wahlwiederholungstaste, wird die gespeicherte Rufnummer automatisch nach 2 Sekunden gewählt. Sollten Sie mehr Zeit zum Lesen der angezeigten Rufnummer benötigen, wählen Sie mit der Bestätigen-Taste "Blättern". Mit jedem Druck auf die Taste "Weiter" wird die nächste der gespeicherten Rufnummern angezeigt. Erst durch Auswählen des Befehls "Anrufen" wird diese Rufnummer gewählt. Dadurch haben Sie wesentlich mehr Zeit zu prüfen, ob die richtige Rufnummer ausgewählt wurde.

Bei einem Anruf über LCR wird nur die vom Teilnehmer gewählte Nummer gespeichert.

PKZ werden ebenfalls im Wahlwiederholungsspeicher abgelegt. Voraussetzung dafür ist das Setzen des entsprechenden systemweiten Flags.

13.1.6.1 Wie Sie die automatische Wahlwiederholung aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **System**.

4) Klicken Sie auf **System Flags**.

5) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie die Funktion aktivieren möchten, aktivieren Sie das Kontrollkästchen **Automatische Wahlwiederholung**.
- Wenn Sie die Funktion deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Automatische Wahlwiederholung**.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

13.1.7 Kurzwahl zentral (KWZ)

Häufig benötigte externe Telefonnummern können im Kommunikationssystem gespeichert werden. Jede Nummer wird dann durch eine Kurzwahlnummer vertreten, die anstelle der vollständigen Telefonnummer benutzt wird.

Kurzwahlnummern bestehen aus 4-stelligen Nummern.

Standardmäßig befindet sich jeder Teilnehmer in einer Gruppe, welcher alle KWZ-Nummern zugeordnet sind. Dadurch darf jeder Teilnehmer alle KWZ-Nummern verwenden.

KWZ setzt die Regeln der Amtsberechtigung außer Kraft.

Die Nummern der zentralen Kurzwahl werden durch den Administrator in Gruppen konfiguriert. Teilnehmer können jeweils einer dieser Gruppen zugeordnet werden. Ein Teilnehmer kann nur die Kurzwahlnummern der ihm zugeordneten Gruppe verwenden. Einer Gruppe kann nur ein KWZ-Bereich zugewiesen werden.

Gewählte Kurzwahlnummern werden in den Wahlwiederholungsspeicher geschrieben.

Zum Programmieren einer Wahlpause und einer MFV-Umschaltung für die Nachwahl von MFV-Zeichen (z. B. für die Steuerung von Sprachboxen) wird die Wahlwiederholungstaste "P-Taste" bzw. die "# -Taste verwendet.

Rufnummernumwertung in Namen

Jedem Kurzwahlziel kann ein Name zugewiesen werden. Sobald eine gespeicherte Rufnummer anruft, setzt das System automatisch den Namen ein und es wird statt der Rufnummer der Name im Display angezeigt, wenn CLIP eingestellt ist.

Nachwahl

Es besteht die Möglichkeit einer Nachwahl:

- Manuelle Nachwahl
  Nach Wahl des Zugangscodes und Angabe der Indexnummer (Kurzwahlnummer) kann der Anwender weitere Ziffern wählen. Diese werden der unter diesem Index gespeicherten Rufnummer angefügt und nachgewählt.
- Automatische Nachwahl
  Bei der Einrichtung einer KWZ kann die eingetragene Nummer in 2 Teile aufgeteilt werden. Als Trennzeichen wird "-" verwendet. Der erste Teil wird auf jeden Fall ausgesendet. Dann wird ein Timer gestartet. Wenn der Benutzer vor Ablauf des Timers keine anderen Ziffern wählt, wird automatisch der zweite Teil der eingetragenen Nummer nachgewählt, ansonsten werden die manuell gewählten Ziffern gesendet.

  Beispiel: KWZ = 7007–0
  Wählt der Teilnehmer nach dem Aufruf der KWZ und vor Ablauf des Timers keine Durchwahl (manuelle Nachwahl), wird automatisch die 0 nachgewählt (automatische Nachwahl).

Import von Kurzwahlrufnummern

Sie können Kurzwahlnummern aus einer XML- oder CSV-Datei im UTF-8-Format importieren. Bereits bestehende Kurzwahlnummern werden vor dem Import gelöscht.

Dateiaufbau:

4-stellige Kurzwahl (führende Nullen verwenden)**;**Amtskennzahl mit Langrufnummer**;** Nachname, Vorname

Beispiel:

```
0001;08970070;Schmidt, Marcus
1010;006768970070;Schmoll, Lucas
```

> ***INFO:*** Eine XML- und eine CSV-Vorlage mit zugehöriger Erklärung finden Sie im WBM unter **Service-Center > Dokumente > CSV-Vorlagen**. In diese Vorlagen können Sie z. B. mit Microsoft Excel Ihre Kurzwahlziele eintragen.

Export von Kurzwahlrufnummern

Als Administrator mit dem Profil **Expert** können Sie über den **Experten-Modus** Kurzwahlnummern in eine XML-Datei im UTF-8-Format exportieren. Es werden immer alle Datensätze exportiert.

13.1.7.1 Wie Sie ein Kurzwahlziel hinzufügen

Mit dem Wizard **Telefonbuch/Kurzwahl** können Sie Kurzwahlziele für Kurzwahl zentral hinzufügen.

Voraussetzungen

- Sie sind am WBM angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Zentrale Telefonie**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Telefonbuch/Kurzwahl** zu starten.

4) Tragen Sie in einer freien Tabellenzeile **Kurzwahl**-Nummer, **Rufnummer** und **Name** des Kurzwahlziels ein.

5) Wenn Sie weitere Kurzwahlziele hinzufügen möchten, klicken Sie auf **Daten speichern** und wiederholen der vorherigen Schritt.

6) Klicken Sie auf **OK & Weiter**.

7) Klicken Sie auf **Beenden**.

13.1.7.2 Wie Sie Kurzwahlziele aus einer XML- oder CSV-Datei importieren

Mit dem Wizard **Telefonbuch/Kurzwahl** können Sie Kurzwahlnummern und Rufnummern aus einer XML- oder CSV-Datei importieren. Bereits bestehende Kurzwahlnummern werden vor dem Import gelöscht.

Voraussetzungen

- Sie sind am WBM angemeldet.
- Eine XML- oder eine CSV-Datei im UTF-8-Format mit eingetragenen Kurzwahlnummern liegt vor. Eine XML- und eine CSV-Vorlage für den Import von Kurzwahlnummern finden Sie unter **Service-Center > Dokumente > CSV-Vorlagen**.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Zentrale Telefonie**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Telefonbuch/Kurzwahl** zu starten. Das Fenster **Zentralen Telefonbucheintrag bearbeiten** wird angezeigt.

4) Klicken Sie auf **CSV/XML-Data importieren/exportieren**.

5) Klicken Sie im Bereich **CSV/XML-Datei über HTTP importieren** auf **Durchsuchen** um die gewünschte Datei auszuwählen.

6) Klicken Sie auf **OK**. Vorhandene Kurzwahlnummern werden gelöscht und die in der XML- oder CSV-Datei eingetragenen Kurzwahlnummern in das System importiert.

7) Klicken Sie auf **Beenden**.

13.1.7.3 Wie Sie Kurzwahlziele in eine XML-Datei exportieren

Sie können Kurzwahlnummern in eine XML-Datei exportieren. Es werden immer alle Daten exportiert.

Voraussetzungen

- Sie sind am WBM angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Zentrale Telefonie**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Telefonbuch/Kurzwahl** zu starten. Das Fenster **Zentralen Telefonbucheintrag bearbeiten** wird angezeigt.

4) Klicken Sie auf **CSV/XML-Data importieren/exportieren**.

5) Klicken Sie im Bereich **XML-Datei über HTTP exportieren** auf **Download**. Die Liste der Kurzwahlnummern wird zum Download vorbereitet.

6) Wählen Sie einen Ablageort für die Datei und klicken Sie auf **Speichern**.

13.1.7.4 Wie Sie Kurzwahlziele bearbeiten

Mit dem Wizard **Telefonbuch/Kurzwahl** können Sie Kurzwahlziele bearbeiten.

Voraussetzungen

- Sie sind am WBM angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Zentrale Telefonie**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Telefonbuch/Kurzwahl** zu starten.

4) Sie können einen Eintrag suchen, indem Sie in die Suchfelder **Kurzwahl**, **Rufnummer** oder **Name** ein Suchbegriff eingegeben und anschließend die Return-Taste drücken. Alle Treffer werden angezeigt, die den Suchbegriff enthalten. Mit der Eingabe von `521` als Rufnummer werden z. B. die Treffer `+495213535` und `+498967521` angezeigt oder mit `co` als Name die Treffer `Collins`, `Mcoin` und `Branco`.

> ***INFO:*** Alle Einträge werden angezeigt, wenn in allen Suchfeldern nichts eingetragen ist und anschließend die Return-Taste gedrückt wird.

5) Ändern Sie in dem gewünschten Tabelleneintrag die Werte in den Feldern **Kurzwahl**, **Rufnummer** oder **Name**.

6) Wenn Sie weitere Kurzwahlziele bearbeiten möchten, klicken Sie auf **Daten speichern** und wiederholen Sie den vorherigen Schritt.

7) Klicken Sie auf **OK & Weiter**.

8) Klicken Sie auf **Beenden**.

13.1.8 Kurzwahl individuell (KWI)

Kurzwahl individuell ermöglicht jedem Teilnehmer zusätzlich zu Kurzwahl zentral 10 externe Rufnummern als individuelle Kurzwahlnummern zu speichern.

Bei Telefonen ohne Display muss der Teilnehmer nach Eingabe der Rufnummer auf den Quittungston warten.

Im KWI-Pool können externe Nummern programmiert werden. Der Zugang hängt von den Wahlberechtigungen des Teilnehmers ab. Der Teilnehmer muss vor Eingabe der Rufnummer die Amtskennzahl (z. B. 0) eingeben.

Um eine Wählpause oder eine MFV-Umschaltung zu programmieren, wird die Taste Wahlwiederholung oder die Raute (#)-Taste verwendet.

13.1.9 Direktruf

Die Funktionstasten eines Telefons oder Beistellgerätes können als Direktruftasten eingerichtet werden. Dafür werden diese mit der Rufnummer eines internen Teilnehmers oder einer Gruppe programmiert. Durch Drücken einer solchen Taste wird ein sofortiger Anruf zum programmierten Ziel ausgeführt (Direktruf). Der aktuelle Zustand des Teilnehmers oder der Gruppe ist anhand der zur Direktruftaste gehörenden LED ersichtlich.

Eine Direktruftaste (auch bezeichnet als DSS (Direct Station Selection)-Taste) kann auch verwendet werden, um ein Gespräch schnell an den darunter programmierten Teilnehmer oder die programmierte Gruppe zu übergeben. Durch das Betätigen einer Direktruftaste während eines Gesprächs mit einem externen Gesprächspartner, wird das aktuelle Gespräch in Rückfrage geschaltet. Der übergebende Teilnehmer kann das Gespräch durch Auflegen des Hörers an das Übergabeziel übergeben (Übergabe vor Melden). Ebenso ist es möglich zu warten, bis das Übergabeziel sich meldet und das Gespräch dann zu übergeben (Übergabe nach Melden). Nimmt das Übergabeziel das Gespräch nicht an, wird ein Wiederanruf veranlasst.

Zustände der zu einer Direktruftaste gehörenden LED

Die zu einer Direktruftaste gehörende LED zeigt den aktuellen Zustand des programmierten Teilnehmers an:

- Aus: Der zugehörige Teilnehmer telefoniert nicht.
- Leuchtet: Der zugehörige Teilnehmer telefoniert oder hat Anrufschutz eingeschaltet.
- Blinkt schnell: Der zugehörige Teilnehmer ruft an. Der Anruf kann durch Drücken der Direktruftaste angenommen werden.
- Blinkt langsam: Der zugehörige Teilnehmer wird gerufen und hat den Anruf noch nicht angenommen. Der Anruf kann durch Drücken der Direktruftaste übernommen werden.

Abhängigkeiten

Thema	Abhängigkeit
ISDN-Telefone, SIP-Telefone	Direktruftasten können nicht bei ISDN- oder SIP-Telefonen programmiert werden.

13.1.10 Direktansprechen / Direktantworten

Direktansprechen ermöglicht einen internen Verbindungsaufbau, ohne dass der gerufene Teilnehmer den Hörer abhebt. Der Lautsprecher des gerufenen Teilnehmers wird dabei automatisch eingeschaltet.

Bei Telefonen mit Freisprecheinrichtung (Mikrofon) ist Direktantworten des gerufenen Teilnehmers durch Einschalten des Mikrofons möglich. Durch Abheben des Hörers erfolgt der Übergang zu einem normalen Zweiergespräch.

Direktansprechen kann mittels einer dafür programmierten Funktionstaste oder über den zugehörigen Menüeintrag oder die Kennzahl und anschließende Wahl der Rufnummer des Zielteilnehmers genutzt werden. Eine Funktionstaste kann auch inklusive einer Teilnehmerrufnummer programmiert werden. Nach Betätigung einer solchen Funktionstaste erfolgt der sofortige Verbindungsaufbau zum programmierten Ziel.

Direktansprechen ermöglicht auch Durchsagen an alle internen Teilnehmer einer Gruppe.

Direktantworten kann über den im Display angebotenen Menüeintrag oder eine dafür programmierte Funktionstaste aktiviert werden.

Das Direktansprechen eines Teilnehmers kann durch Aktivieren des Direktansprechschutzes verhindert werden. In diesem Fall wird das Direktansprechen wie ein normaler Anruf signalisiert.

Abhängigkeiten

Thema	Abhängigkeit
Anrufschutz, Anrufschutz durchbrechen	Bei Teilnehmern mit aktiviertem Anrufschutz ist kein Direktansprechen möglich. Hat der Teilnehmer, der das Leistungsmerkmal "Direktansprechen" nutzen möchte, die Berechtigung den Anrufschutz zu durchbrechen, erhält dieser für fünf Sekunden den Besetztton. Anschließend wird der Zielteilnehmer gerufen, nicht direkt angesprochen.
Makeln, Rückfrage Übergabe	Die genannten Leistungsmerkmale können nicht in einer Direktansprechen/Direktantworten-Verbindung genutzt werden.
ISDN-Telefone, SIP-Telefone	Die Leistungsmerkmale "Direktansprechen" und "Direktantworten" können nicht mit ISDN- oder SIP-Telefonen genutzt werden.

13.1.10.1 Wie Sie den Direktansprechschutz für Teilnehmer aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Teilnehmer**.

3) Navigieren Sie im Menübaum unter **Teilnehmer > Teilnehmer > ...** zum gewünschten Teilnehmer (Index-Rufnummer-Name).

4) Klicken Sie auf die Registerkarte **Teilnehmer-Flags ändern**.

5) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie den Direktansprechschutz für Teilnehmer aktivieren möchten, deaktivieren Sie das Kontrollkästchen **Direktansprechschutz aus**.
- Wenn Sie den Direktansprechschutz für Teilnehmer deaktivieren möchten, aktivieren Sie das Kontrollkästchen **Direktansprechschutz aus**.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

13.1.11 Assoziierte Wahl

Assoziierte Wahl ermöglicht einem berechtigten Teilnehmer für einen beliebigen anderen Teilnehmer stellvertretend eine Rufnummer zu wählen. Die Auswirkung ist die gleiche, wie bei der Wahl der Rufnummer durch den anderen Teilnehmer selbst.

Der Einstieg erfolgt über eine Kennzahl mit Angabe des Teilnehmers, für den die Wahl ausgeführt werden soll. Die nachfolgenden Ziffern werden dabei so interpretiert, als ob der zuvor angegebene Teilnehmer selbst wählen würde.

13.1.12 Leitungsvormerken

Ein Teilnehmer kann sich eine Amtsleitung vormerken, wenn momentan keine freie Amtsleitung zur Verfügung steht. Sobald eine Amtsleitung frei wird, bekommt er diese mittels Wiederanruf angeboten.

Wenn der Teilnehmer zum Zeitpunkt des Wiederanrufs belegt ist, wird beim besetzten Teilnehmer angeklopft. Wird das Anklopfen nicht beantwortet, wird die Reservierung gelöscht und die Leitung dem nächsten Teilnehmer in der Warteliste angeboten. Hat der Teilnehmer vor Eingang eines Wiederanrufs von einer in der Warteliste befindlichen Amtsleitung den Anrufschutz aktiviert, wird die Leitungsreservierung gelöscht und die Amtsleitung dem nächsten Teilnehmer in der Warteliste angeboten.

Merken mehrere Teilnehmer eine Amtsleitung vor, so erfolgt die Zuteilung in der Reihenfolge der Vormerkung.

Pro Telefon ist nur eine Warteliste-/Reservierungsanforderung möglich. Wenn der Teilnehmer eine zweite Reservierung versucht, wird die erste dadurch überschrieben.

Es ist nicht möglich, das Leistungsmerkmal Leitungsvormerken zu aktivieren, wenn die versuchte Verbindung über LCR (Leitweglenkung) eingeleitet wurde.

Das Leistungsmerkmal Leitungsvormerken ignoriert eine vorhandene Rufweiterschaltung. Erfolgt innerhalb von 20 Sekunden keine Antwort, wird die Leitungsreservierung gelöscht.

Eine wieder anrufende Amtsleitung kann nicht übernommen werden – weder durch "Übernahme, gezielt" noch durch "Übernahme, Gruppe".

Die Reservierung der Leitungen kann auf einem der folgenden Wege aktiviert werden:

- Manuelle Reservierungen funktionieren nur bei Telefonen mit Display.
- Automatische Reservierung (bei allen anderen Telefonen)
  Wenn dieses Flag aktiviert ist und einem Teilnehmer nach den üblichen Prozeduren zur Leitungsbelegung keine freie Leitung zugewiesen wird, wird teilnehmerseitig ein Besetztton signalisiert. Nach 5 Sekunden ertönt ein positiver Quittungston und die Leitung wird reserviert, sofern der Teilnehmer über die erforderliche Amtsrufberechtigung verfügt.

INFO: Bei S_0-Telefonen Leistung vormerken nicht möglich.

13.1.12.1 Wie Sie Leitungsvormerken aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **System**.

4) Klicken Sie auf **System Flags**.

5) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie die Funktion aktivieren möchten, aktivieren Sie das Kontrollkästchen **automatisches Leitungsvormerken**.
- Wenn Sie die Funktion deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **automatisches Leitungsvormerken**.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

13.1.13 Privatleitung

Einer Privatleitung ist eine Amtsleitung, die ausschließlich einem bestimmten Teilnehmer zur Verfügung steht.

13.2 Anrufsignalisierung, Rufnummernanzeige

Das Kommunikationssystem bietet verschiedene Möglichkeiten der Anrufsignalisierung und Rufnummernanzeige, wie z. B. CLIP, CLIR, COLP und COLR.

13.2.1 Unterschiedliche Anrufsignalisierung

Unterschiedliche Anrufsignalisierung ermöglicht bei ankommenden Anrufen zwischen internen und externen zu unterscheiden.

Kommende Anrufe werden am Telefon optisch und akustisch signalisiert. Im Display erscheinen folgende Anzeigen:

- Rufnummer des Anrufers
- bei interner Anrufumleitung: zusätzlich die eigentlich gewählte Rufnummer

Der kommende Anruf kann zusätzlich durch eine LED angezeigt werden. Für interne und externe Anrufe gibt es unterschiedliche akustische Signale.

Rufsignalisierung intern

Es kann jedem Teilnehmer eine von insgesamt acht möglichen akustischen Rufsignalisierungen für interne Anrufe zugewiesen werden. Dadurch sendet der Teilnehmer anderen internen Teilnehmern einen veränderten Rufton, durch den er von anderen unterschieden werden kann. So kann z. B. dem Geschäftsführer ein spezieller interner Rufton bereitgestellt werden und jeder Mitarbeiter erkennt bereits am Rufton, dass er vom Geschäftsführer angerufen wird.

Rufsignalisierung extern

Es gibt drei verschiedene Rufarten, die sich akustisch unterscheiden und für einen externen Ruf eingestellt werden können. Dadurch können z. B. Anrufe für zwei verschiedene Gruppen wie Vertrieb und Lager akustisch unterschieden werden.

- Durch den Administrator werden die drei unterschiedlichen Rufarten in Deutschland für analoge, ISDN- und System-Telefone konfiguriert.
- In anderen Ländern werden die Rufarten von analogen Telefonen gleich signalisiert.

13.2.2 Rufnummernübermittlung des Anrufers (CLIP)

Rufnummernübermittlung des Anrufers zeigt die Rufnummer des Anrufers beim gerufenen Teilnehmer an.

Die Rufnummernübermittlung des Anrufers CLIP (Calling Line Identification Presentation) bezieht sich auf ankommende Rufe und muss vom Netzanbieter unterstützt werden.

Ist der Name und die Rufnummer des Anrufers unter Kurzwahl zentral (KWZ) des Kommunikationssystems gespeichert, sehen Sie den Namen auf Ihrem Display.

Die Leistungsmerkmale Rufnummernübermittlung des Anrufers (CLIP) und Rufnummernunterdrückung des Anrufers (CLIR) schließen einander gegenseitig aus, d. h. sobald CLIP aktiviert ist, ist CLIR deaktiviert und umgekehrt.

Einstellbare CLIP

Einstellbare CLIP überträgt nach extern anstelle der Rufnummer des Anrufers (z. B. Mitglied eines Sammelanschlusses) eine dafür eingestellte Rufnummer (z. B. Rufnummer des Sammelanschlusses).

Systemspezifische Informationen

Land	standardmäßig aktiviert
USA	LIN (Location Identification Number). Wird CLIP für USA aktiviert, ist LIN automatisch deaktiviert.
restliche Länder	CLIP

13.2.2.1 Wie Sie einstellbare CLIP aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **System**.

4) Klicken Sie auf **System Flags**.

5) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie einstellbare CLIP aktivieren möchten, aktivieren Sie das Kontrollkästchen **Einstellbare CLIP**.
- Wenn Sie einstellbare CLIP deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Einstellbare CLIP**.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

13.2.3 Rufnummernunterdrückung des Anrufers (CLIR)

Rufnummernunterdrückung des Anrufers unterdrückt die Anzeige der Rufnummer des Anrufers beim angerufenen Teilnehmer.

Rufnummernunterdrückung CLIR (Calling Line Identification Restriction) bezieht sich auf gehende Anrufe. PSTN muss das Leistungsmerkmal unterstützen. Rufnummernunterdrückung hat Vorrang vor Rufnummernübermittlung.

Die Leistungsmerkmale Rufnummernübermittlung des Anrufers (CLIP) und Rufnummernunterdrückung des Anrufers (CLIR) schließen einander gegenseitig aus, d. h. sobald CLIP aktiviert ist, ist CLIR deaktiviert und umgekehrt.

CLIR und COLR können nur gemeinsam aktiviert oder deaktiviert sein.

Rufnummernunterdrückung des Anrufers ist für bestimmte Anrufziele (z. B. Notrufnummern von Polizei und Feuerwehr) nicht wirksam.

Systemweite Rufnummernunterdrückung

Als Administrator können Sie CLIR Rufnummernanzeige systemweit aktivieren oder deaktivieren.

INFO: Das Flag “Systemweite Unterdrückung der Rufnummernanzeige” gilt nicht für USA.

Temporäre Rufnummernunterdrückung

Als Teilnehmer können Sie die temporäre Rufnummernunterdrückung aktivieren oder deaktivieren. Temporäre Rufnummernunterdrückung ist nur möglich bei deaktivierter systemweiter Rufnummernunterdrückung.

Teilnehmerrufnummer unterdrücken

Als Administrator können Sie bezogen auf jeweils eine Richtung konfigurieren, dass anstelle der Rufnummer des Teilnehmers nur Anlagenrufnummer übertragen werden soll.

13.2.3.1 Wie Sie die Unterdrückung der Teilnehmerrufnummer aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Leitungen Vernetzung**.

3) Klicken Sie im Menübaum auf **Richtung**.

4) Wählen Sie die betreffende **Rtg.** aus.

5) Aktivieren Sie unter **Anlagenrufnummer gehend** das Kontrollkästchen **TIn-RufNr unterdrücken**.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

13.2.4 Rufnummernübermittlung des Angerufenen (COLP)

Rufnummernübermittlung des Angerufenen übermittelt dem Anrufer die Rufnummer des angerufenen Teilnehmers, sobald die beiden verbunden sind.

Rufnummernübermittlung des Angerufenen (COLP Connected Line Identification Presentation) ist ein ISDN-Leistungsmerkmal.

COLP ist z. B. bei einer Anrufumleitung sinnvoll, damit der Anrufer an Stelle der gewählten Rufnummer diejenige seines Gesprächspartners sieht.

Die Leistungsmerkmale Rufnummernübermittlung des Angerufenen (COLP) und Rufnummernunterdrückung des Angerufenen (COLR) schließen einander gegenseitig aus, d. h. sobald COLP aktiviert ist, ist COLR deaktiviert und umgekehrt.

13.2.4.1 Wie Sie die Rufnummernübermittlung des Angerufenen aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Leitungen Vernetzung**.

3) Klicken Sie im Menübaum auf **Richtung**.

4) Wählen Sie die entsprechende **Rtg.** aus.

5) Klicken Sie auf die Registerkarte **Spezial Parameter ändern**.

6) Aktivieren Sie das Kontrollkästchen **COLP**.

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

13.2.5 Rufnummernunterdrückung des Angerufenen (COLR)

Rufnummernunterdrückung des Angerufenen unterdrückt die Anzeige der Rufnummer des angerufenen Teilnehmer beim Anrufer.

Rufnummernunterdrückung des Angerufenen (COLR Connected Line Identification Restriction) bezieht sich auf kommende Anrufe.

Rufnummernunterdrückung des Angerufenen (COLR) hat Vorrang vor Rufnummernübertragung des Angerufenen beim Anrufer.

Die Leistungsmerkmale Rufnummernübermittlung des Angerufenen (COLP) und Rufnummernunterdrückung des Angerufenen (COLR) schließen einander

gegenseitig aus, d. h. sobald COLP aktiviert ist, ist COLR deaktiviert und umgekehrt.

CLIR und COLR können nur gemeinsam aktiviert oder deaktiviert sein.

13.2.6 CLIP no screening (Übermittlung kundenspezifischer Rufnummerninformationen)

CLIP no screening übermittelt an Stelle der Rufnummer des Anrufers eine vom Anrufer festgelegte Rufnummer.

Die Anlagenrufnummer gehend muss nicht identisch sein mit der Anlagenrufnummer kommend.

Für spezielle Kundenanwendungen kann das Flag "Teilnehmerrufnummer unterdrücken" aktiviert werden. Dadurch wird verhindert, dass die Durchwahlnummer des Teilnehmers mit der Anlagenrufnummer gehend ausgesendet wird.

Beispiel: Ein Service-Mitarbeiter, der zentral über eine allgemeine Service-Rufnummer erreicht wird, soll von seinen Kunden nicht direkt erreicht werden können. Um seine eigene Durchwahlnummer zu verbergen, wird als Anlagenrufnummer gehend die allgemeine Service-Rufnummer eingetragen und das Flag "Teilnehmerrufnummer unterdrücken" aktiviert. Dem angerufenen Teilnehmer wird dann ausschließlich die allgemeine Service-Rufnummer als CLIP angezeigt.

Im Normalfall wird für kommende und gehende Gespräche dieselbe Anlagenrufnummer verwendet. Der Eintrag unter Anlagenrufnummer gehend ist dann leer oder identisch mit dem unter Anlagenrufnummer kommend. Soll dies nicht der Fall sein, kann

- unter Anlagenrufnummer gehend eine andere Nummer eingetragen werden.
- über den Richtungsparameter Nr.-Typ, gehend definiert werden, ob die eingetragene Anlagenrufnummer gehend die Teilnehmernummer ohne Ortsnetzkennzahl, mit Ortsnetzkennzahl (national) oder zusätzlich die internationale Länderkennzahl (international) enthält.

> ***INFO:*** CLIP no screening muss vom Netzanbieter unterstützt werden und aktiviert sein.

13.2.6.1 Wie Sie CLIP no screening konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Leitungen Vernetzung**.

3) Klicken Sie im Menübaum auf **Richtung**.

4) Wählen Sie die betreffende **Rtg.** aus.

5) Geben Sie unter **Anlagenrufnummer gehend** die gewünschte **Anlagenrufnummer** ein.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

13.2.7 CLIP für analoge Endgeräte

CLIP für analoge Endgeräte übermittelt die Rufnummer von einem analogen Endgerät des Anrufers zum Angerufenen und die dortige Anzeige auf dafür geeigneten Endgeräten – CLIP (Calling Line Identification Presentation) analog.

Die zusätzliche Übertragung der Namensinformation CNIP (Calling Name Identification Presentation) ist konfigurierbar.

INFO: CNIP ist endgeräteabhängig. Beachten Sie die Angaben des Herstellers.

13.2.8 Stiller Ruf / Ruhe

Das Leistungsmerkmal Stiller Ruf / Ruhe signalisiert kommende Rufe akustisch nur mit einem kurzen Aufmerksamkeitston und im Display.

Stiller Ruf / Ruhe ist nur an Telefonen mit Display verfügbar und hat keine Auswirkung auf die Signalisierung von Terminen.

13.2.9 Rufnummernumwertung in Namen bei Kurzwahl zentral

Bei Anrufen mittels Kurzwahl zentral (KWZ) und bei ankommenden Anrufen von Zielen der Kurzwahl zentral, wird nach der Wahl anstelle der Kurzwahlnummer der Name des Kurzwahlzieles angezeigt.

13.3 Funktionen während der Verbindung

Das Kommunikationssystem bietet während der Verbindung verschiedene Funktionen an, z. B. Gespräch halten, weiterleiten oder übergeben.

13.3.1 Halten

Mit Halten bringt ein Teilnehmer ein Gespräch in einen Wartezustand. Der Anrufer hört währenddessen Wartemusik oder eine Ansage.

Halten wird beendet durch die Wiederaufnahme des gehaltenen Gesprächs.

Es gibt folgende Arten von Halten:

- allgemeines Halten:
  Jeder beliebige Teilnehmer kann das Gespräch durch Drücken einer Leitungs- oder Gesprächstaste wieder aufnehmen.
- exklusives Halten: (nur bei Team- oder Top-Funktion und beim Vermittlungsplatz)
  Nur der zuvor einleitende Teilnehmer kann das Gespräch wieder aufnehmen.

Halten und Wiederanruf

Ein geparktes Gespräch führt bei Ablauf des Timers **Zeit für Parken + Übergang Halten** (Standard 160 s) zu einem Wiederanruf.

13.3.2 Parken

Mit Parken bringt ein Teilnehmer ein Gespräch in einen Wartezustand. Der Anrufer hört währenddessen Wartemusik oder eine Ansage. Ein geparktes Gespräch kann von einem beliebigen Telefon aus wieder aufgenommen werden.

Als Teilnehmer weisen Sie einer zu parkenden Verbindung eine Parkposition (0-9) im Kommunikationssystem zu. Ist die Parkposition belegt, ertönt ein negativer Quittungston, die Ziffer wird nicht dargestellt und Sie können eine andere Parkposition wählen. Zur Wiederaufnahme eines geparkten Gesprächs müssen Sie dessen Parkposition angeben.

Die Wiederaufnahme eines geparkten Gesprächs kann über Kennzahl oder eine entsprechend programmierte Taste erfolgen und ist auch während eines anstehenden Rufs möglich.

Parken und Wiederanruf

Ein geparktes Gespräch führt bei Ablauf des Timers **Zeit für Parken + Übergang Halten** (Standard: 160 s) zu einem Wiederanruf.

Parken und Anrufumleitung

Ein geparktes Gespräch folgt bei einem Wiederanruf nicht einer Anrufumleitung.

Parken und DISA

Parken kann nicht über DISA aktiviert werden.

Parken und Konferenz

Eine Konferenz kann nicht geparkt werden.

Parken und Vernetzung

Ein geparkter Anruf kann nur im gleichen Knoten wieder aufgenommen werden. Ein über Vernetzung kommender Anruf kann nur am Zielknoten geparkt werden.

Parken und Anrufschutz

Ein Teilnehmer mit aktiviertem Anrufschutz kann einem Gespräch eine Parkposition zuweisen. Erfolgt ein Wiederanruf durch das geparkte Gespräch und wurde in Call Management kein anderes Ziel festgelegt, wird das Gespräch nach Ablauf des Wiederanruf-Timers automatisch getrennt.

13.3.3 Rückfrage

Mit Rückfrage baut ein Teilnehmer während eines Gesprächs ein weiteres Gespräch vom selben Telefon aus auf oder nimmt ein anklopfendes Gespräch an. Das erste Gespräch wird währenddessen gehalten.

Eine Rückfrage wird beendet durch:

- Wiederaufnahme des gehaltenen Gesprächs
- Trennen
  Dadurch erfolgt entweder:
  - Übergabe des gehaltenen Gesprächs oder
  - sofortiger Wiederanruf des gehaltenen Teilnehmers beim Teilnehmer, der die Verbindung getrennt hat

Rückfrage mittels Direktruftaste

Das Drücken einer Direktruftaste während eines Gesprächs leitet eine Rückfrage zum entsprechenden Ziel ein.

Verbinden zweier externer Gesprächspartner

Während eines externen Gesprächs verbindet eine Rückfrage zu einem externen Ziel bei anschließender Übergabe die beiden Gesprächspartner. Dabei können Gebühren anfallen.

13.3.4 Makeln

Mit Makeln kann ein Teilnehmer zwischen zwei Gesprächen wechseln. Während er mit einem der Teilnehmer im Gespräch ist, wird der jeweils andere gehalten.

Teilnehmer können durch Drücken der entsprechenden Leitungstaste zwischen den Gesprächen wechseln.

Makeln und Halten

Ein gehaltener Teilnehmer kann nicht makeln.

13.3.5 Übergabe

Mit Übergabe kann ein Teilnehmer sein Gespräch an ein anderes Ziel übergeben. Sobald ein Teilnehmer die Übergabe einleitet, wird der wartende Teilnehmer bis auf weiteres gehalten.

Es gibt folgende Arten von Übergabe:

- Übergabe vor Melden:
  Sie können den Anruf übergeben, ohne dass sich der Teilnehmer am Ziel der Übergabe meldet. Falls der Teilnehmer am Ziel der Übergabe besetzt ist, wird angeklopft. Versucht noch ein Dritter diesem besetzten Teilnehmer ein Gespräch zu übergeben oder ist Anklopfschutz aktiviert, erfolgt ein sofortiger Wiederanruf. Beantwortet der Teilnehmer am Ziel das übergebene Gespräch nicht innerhalb einer bestimmten Zeit (Timer Rufzeit während Übergeben vor Melden), erfolgt Wiederanruf. Übergabe vor Melden ist nicht möglich an einen Agenten einer anderen Warteschlange von Multimedia Contact Center.
- Übergabe nur mit Rückfrage:
  Sie können den Anruf erst übergeben, wenn sich der Teilnehmer am Ziel der Übergabe meldet. Sie übergeben den Anruf durch Auflegen des Hörers.

Übergabe bei Anrufumleitung

Einer Anrufumleitung am Ziel der Übergabe wird gefolgt. Das Display zeigt das letztendliche Ziel der Übergabe.

Übergabe bei Anrufschutz

Bei der Übergabe eines Gesprächs an einen Teilnehmer mit aktiviertem Anrufschutz erfolgt sofort ein Wiederanruf beim einleitenden Teilnehmer, unabhängig von dessen Anrufschutz.

Systemspezifische Informationen

Timer Rufzeit während Übergeben vor Melden: standardmäßig 45 s

An einen besetzten Teilnehmer können gleichzeitig bis zu 5 Gespräche übergeben werden.

13.3.6 Wiederanruf

Mit Wiederanruf erhält der einleitende Teilnehmer automatisch ein zu lange gehaltenes, zu lange geparktes Gespräch oder ein nicht erfolgreich übergebenes Gespräch erneut.

Wiederanruf erfolgt in folgenden Fällen:

- Ein gehaltenes oder geparktes Gespräch wird nicht innerhalb einer bestimmten Zeit wieder aufgenommen (Timer Zeit für Parken + Übergang Halten).
- Bei Übergabe vor Melden unter folgenden Umständen:

- wird nicht beantwortet vor Ablauf einer bestimmten Zeit (Timer Rufzeit während Übergeben vor Melden)
- Ziel existiert nicht
- Ziel ist zweitgradig besetzt
- digitales Telefon am Ziel ist defekt
- Übergabe ist nicht zulässig

Ist der einleitende Teilnehmer während des Wiederanrufs besetzt, klopft der Wiederanruf an. Sobald der einleitende Teilnehmer wieder frei ist, wird der Wiederanruf signalisiert. Im Display des einleitenden Teilnehmers kann entweder die Rufnummer des Anrufers oder des Zielteilnehmers angezeigt werden. Beantwortet der Teilnehmer den Wiederanruf nicht bis zum Ablauf des Timers Abwurfzeit für Wiederanruf, erfolgt Abwurf an den Abwurfplatz, wenn das Flag bei nichtbeantwortetem Wiederanruf gesetzt ist. Beantwortet der Abwurfplatz den Wiederanruf nicht bis zum Ablauf des Timers Zeit für das Auslösen eines Wiederanrufes am VPL, wird der Wiederanruf automatisch getrennt.

Wiederanruf und Anrufübernahme

Jeder Teilnehmer in einer Anrufübernahmegruppe mit dem einleitenden Teilnehmer kann einen Wiederanruf übernehmen, wenn das systemweite Flag AUN nach Wiederanruf gesetzt ist.

Wiederanruf und Anrufschutz

Ein Wiederanruf ignoriert Anrufschutz.

Systemspezifische Informationen

Timer Abwurfzeit für Wiederanruf: standardmäßig 30 s

Timer Zeit für das Auslösen eines Wiederanrufes am VPL: standardmäßig 60 s

13.3.7 Call Monitoring (nur ausgewählte Länder)

Call Monitoring ermöglicht berechtigten Teilnehmern ein Gespräch eines beliebigen internen Teilnehmers mitzuhören. Das Mikrofon des mithörenden Teilnehmers wird automatisch stummgeschaltet. Die Teilnehmer der überwachten Verbindung erhalten keinerlei Hinweis auf den Vorgang, wie z. B. Ton oder Displayanzeige.

Das Leistungsmerkmal kann ausschließlich in folgenden Ländern genutzt werden: Argentinien, Australien, Belgien, Brasilien, Frankreich, Großbritannien, Hongkong, Indien, Irland, Malaysia, Neuseeland, Niederlande, Portugal, Singapur, Spanien, Südafrika, Thailand, USA.

Berechtigte Teilnehmer benötigen ein Systemtelefon und die Berechtigung für Aufschalten.

Der zu überwachende Teilnehmer muss sich in einem aktiven Gesprächszustand befinden. Beim Beginn und beim Beenden des Call Monitoring können Gesprächsaussetzer von bis zu zwei Sekunden auftreten. Sobald einer der Gesprächsteilnehmer in der überwachten Verbindung gehalten wird, übergeben wird oder das

Gespräch beendet, wird die Mithörverbindung getrennt. Die Mithörverbindung kann erst dann wiederhergestellt werden, wenn sich der zu überwachende Teilnehmer wieder in einem aktiven Gesprächszustand befindet.

Abhängigkeiten

Thema	Abhängigkeit
Schnurlose Telefone	Sie können Call Monitoring nicht an einem schnurlosen Telefon verwenden, da dieses die automatische Mikrofon-Stummschaltung nicht unterstützt.
Konferenz	Call Monitoring schränkt die mögliche Anzahl an Konferenzen ein. Maximale Anzahl möglicher Konferenzen im System = maximale Anzahl gleichzeitiger Call-Monitoring-Teilnehmer.

13.3.7.1 Wie Sie Call Monitoring für einen Teilnehmer aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.
- Für den betreffenden Teilnehmer ist die Aufschalteberechtigung aktiviert.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Teilnehmer**.

3) Klicken Sie im Menübaum auf **Teilnehmer**.

4) Navigieren Sie im Menübaum unter **Teilnehmer > Teilnehmer > ...** zum gewünschten Teilnehmer (Index - Rufnummer - Name).

5) Klicken Sie auf die Registerkarte **Teilnehmer-Flags ändern**.

6) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie die einem Teilnehmer die Berechtigung für diese Funktion erteilen möchten, aktivieren Sie das Kontrollkästchen **Call Monitoring**.
- Wenn Sie die einem Teilnehmer die Berechtigung für diese Funktion entziehen möchten, deaktivieren Sie das Kontrollkästchen **Call Monitoring**.

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

13.3.8 Diskretes Ansprechen

Das Leistungsmerkmal Diskretes Ansprechen ermöglicht es einem Teilnehmer C bei einer einfachen Verbindung zwischen den zwei Teilnehmern A und B mitzuhören und Teilnehmer A Hinweise zu geben, welche für Teilnehmer B nicht hörbar sind, typischerweise in Callcentern oder bei Chef-/Sekretär-Anlagen.

Das Leistungsmerkmal ist in Manager E zu konfigurieren.

> ***INFO:*** Obwohl es keine Verbindung zwischen Teilnehmer B und Teilnehmer C gibt, kann Teilnehmer B über Rückkopplung beim Telefon von Teilnehmer A eventuell doch gedämpft hören was Teilnehmer C spricht.

Zielendgeräte für das diskrete Ansprechen (Teilnehmer A) können nur Systemtelefone mit Display sein. Die Teilnehmer A und C müssen im selben Knoten sein.

Das Leistungsmerkmal wird von Teilnehmer C im Ruhe/Bereit-Zustand durch Wahl einer Kennzahl aktiviert. Es gibt eine teilbelegte Taste (nur die Kennzahl liegt auf der Taste, die Rufnummer muss nachgewählt werden) am Telefon. Im Servicemenü wird ein Menüpunkt eingebracht, das Idle/Gesprächs-Menü bleibt unverändert.

Die Möglichkeit das Feature zu aktivieren ist an eine benutzerspezifische Berechtigung geknüpft. Mit einer zweiten Berechtigung kann sich Teilnehmer A vor dem diskreten Ansprechen schützen.

Die Deaktivierung erfolgt entweder durch Auslösen des aktivierenden Teilnehmers C oder durch Leistungsmerkmalbeeinflussung.

> ***INFO:*** Ist nicht mindestens ein Teilnehmer des ursprünglichen Gesprächs ein TDM-Teilnehmer, so ist zum Zeitpunkt des Aktivierens das Koppelfeld noch nicht beteiligt und das Umschalten kann nicht ohne kurzzeitige Unterbrechung der bisherigen Verbindung durchgeführt werden.

Ist das Leistungsmerkmal Diskretes Ansprechen aktiv und Teilnehmer A oder Teilnehmer B leitet ein anderes verbindungsbezogenes Leistungsmerkmal ein, so wird Diskretes Ansprechen prinzipiell beendet. Details zum Verhalten bei bestimmten Leistungsmerkmalen siehe folgende Tabelle:

Leistungsmerkmal	**Teilnehmer A**		**Teilnehmer B**		**Teilnehmer C**	
	Möglich	Aktion	Möglich	Aktion	Möglich	Aktion
Rückfrage, Halten, Parken, Gemeinsames Halten	Ja	„Diskretes Ansprechen“ beenden	Ja	„Diskretes Ansprechen“ beenden	Nein	Negativ quittieren
Übergeben	--	--	--	--	--	--
Konferenz	--	--	--	--	--	--
Anklopfen	Ja	--	Ja	--	Ja	--

Leistungsmerkmal	Teilnehmer A		Teilnehmer B		Teilnehmer C	
Anklopfen annehmen	Ja	„Diskretes Ansprechen“ beenden	Ja	„Diskretes Ansprechen“ beenden	Ja	Negativ quittieren
Aufschalten	Nein	--	Nein	--	Nein	--
DTMF Übertragung	Ja	--	Ja	--	Nein	--
LM-Zähler	--	--	--	--	--	--
Assoziierte Dienste	--	--	--	--	--	--
DISA / DISI	--	--	--	--	--	--

13.4 Steuern der Erreichbarkeit

Zum Steuern der Erreichbarkeit bietet das System Leistungsmerkmale wie Anrufumleitung, Anrufschutz und Abweisen von Anrufen.

Verschiedene Arten von Anrufumleitungen benutzen Rufziellisten. Rufziellisten legen fest, wie ankommende Rufe für den zugeordneten Teilnehmer bzw. die zugeordnete Gruppe behandelt werden. Ziele in einer Rufzielliste werden nacheinander abgearbeitet. Unterschiedliche Einträge für Intern- und Externrufe (Tag bzw. Nacht) sind möglich.

13.4.1 Rufweiterschaltung

Die Rufweiterschaltung leitet Anrufe weiter, wenn sie nicht innerhalb einer bestimmten Zeit angenommen werden.

Diese Art der Rufweiterschaltung wird auch als Feste Rufweiterschaltung bezeichnet, weil Sie nur durch den Administrator konfigurierbar ist.

Für jede Rufweiterschaltung gibt es eine oder mehrere Rufziellisten, die den Teilnehmern für folgende Arten von Anrufen zugeordnet werden können:

- externe Anrufe tagsüber (während inaktiver Nachtschaltung)
- externe Anrufe nachts (während aktiver Nachtschaltung)
- interne Anrufe

Pro Rufzielliste können Sie bis zu 4 Rufziele angeben, an die der Anruf nach Ablauf einer einstellbaren Zeit der Reihe nach weitergeschaltet wird.

Beim Rufziel werden Rufnummer oder Name des ursprünglich gerufenen Teilnehmers und Rufnummer oder Name des Anrufers angezeigt. Die zusätzliche Anzeige der Rufnummer oder des Namens des Anrufers können Sie als Administrator deaktivieren.

Rufweiterschaltung im Besetztfall

Die Rufweiterschaltung im Besetztfall leitet einen ankommenden Anruf bei einer besetzten Nebenstelle sofort zum nächsten Rufziel weiter.

Ist das Rufziel ebenfalls besetzt, wird dem Anrufer besetzt signalisiert. Bei einem internen Anruf bleibt der Anruf in diesem Fall beim Rufziel, das zyklisch auf Freiwerden geprüft wird. Der Administrator legt den Zyklus fest.

Ist das Rufziel nicht verfügbar und ist hierfür keine weitere Rufweiterschaltung eingerichtet, wird der Anruf nicht weitergeschaltet.

Abhängigkeiten

Thema	Abhängigkeit
Analoge Telefone	Bei diesen Telefonen ist nicht zu erkennen, dass es sich bei dem eingehenden Ruf um einen weitergeleiteten Ruf handelt.
Anklopfen	Hat ein Teilnehmer Anklopfen freigegeben, wird bei ihm auch dann angeklopft, wenn für ihn Rufweiterschaltung im Besetztfall konfiguriert ist.
Anklopfschutz	Ein Rufziel, das den Anklopfschutz aktiviert hat, wird übersprungen.
Anrufumleitung AUL	Eine Rufweiterschaltung wird erst ausgeführt, wenn nach einer vom Administrator eingestellten Zeit das Ziel einer Anrufumleitung nicht antwortet.
Nachtschaltung	Wird für einen Teilnehmer in der Rufweiterschaltung die Möglichkeit "tagsüber / nachts" verwendet und die Nachtschaltung aktiviert, werden externe Anrufe entsprechend der Einstellung bei Nachtschaltung umgeleitet. Interne Anrufe folgen weiterhin der Einstellung "tagsüber".
Rufweiterschaltung ins Amt	Ist eine Rufweiterschaltung ins Amt aktiviert, so hat diese Vorrang vor anderen Rufweiterschaltungen.
Sammelanschluss / Gruppenruf	Wird eine Gruppe oder ein Sammelanschluss als Ziel einer Rufweiterschaltung eingetragen, so wird diese Gruppe erst vollständig abgearbeitet, d. h. nacheinander gerufen, bevor das nächste Ziel der Rufweiterschaltung ausgewertet wird. Gruppenruf und Sammelanschluss sind wie eine Rufweiterschaltung innerhalb der Rufweiterschaltung anzusehen. Ein Sammelanschluss ist besetzt, wenn alle Mitglieder besetzt sind oder sich aus dem Sammelanschluss herausgeschaltet haben. Eine Gruppe ist immer dann besetzt, wenn alle Gruppenmitglieder besetzt sind.

13.4.1.1 Wie Sie eine Rufweiterschaltung konfigurieren

Mit dem Wizard **Rufweiterschaltung** konfigurieren Sie für interne Teilnehmer eine Rufweiterschaltung bei ankommenden Anrufen.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > User Telefonie**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Rufweiterschaltung** zu starten. Es öffnet sich das Fenster **Rufzielliste - Definition**.

4) Definieren Sie zuerst eine Rufzielliste, indem Sie in der Zeile der zu bearbeitenden Rufzielliste auf das Symbol **Bearbeiten** klicken.

5) Wählen Sie in den Aufklapplisten **1. Ziel** bis **4. Ziel** die gewünschten Ziele aus. Sie haben folgende Möglichkeiten:

- **Kein Eintrag**: Ziel wird übersprungen
- **Externes Ziel**: Richtung und externe Rufnummer mit Amtskennzahl
- *** Angewählter Teilnehmer**: der angerufene Teilnehmer
- **** Benutzer definiert**: Ziel der Anrufumleitung nach Zeit (falls eingerichtet).
- **#9 Systemsuchlauf**: nächster verfügbarer Teilnehmer (außer Chef-Nebenstelle)
- **#201 - #260**: Anrufverteilung (UCD-Gruppe)
- **#801 - #817**: Ansagegerät
- **100, 101, ...**: Rufnummer eines internern Teilnehmers oder einer Gruppe (z. B. Sprachbox)

INFO: Um ein Rufziel schneller zu finden, können Sie in den Feldern **1. - 4. Ziel** auch eine oder mehrere Ziffern eingeben. Dann wird direkt zum Listeneintrag gesprungen, der mit der eingegebenen Ziffernfolge beginnt. Die Eingabe einer Buchstabenfolge ist ebenfalls möglich.

---

6) Wählen Sie in der Aufklappliste
Die Rufweiterschaltung erfolgt immer nach die Zeit in Sekunden aus, nach der ein Anruf an das nächste Ziel weitergeschaltet wird.

7) Aktivieren Sie das Kontrollkästchen **Rufweiterschaltung**, wenn der Anruf im Besetztfall sofort an das nächste Rufziel weitergeleitet werden soll.

8) Wenn der Anruf bei einem zusätzlichen internen Teilnehmer signalisiert werden soll oder z. B. bei einem Relais (Aktor) für einen zentralen Wecker, wählen Sie in der Aufklappliste **Zweitwecker Ziel** die gewünschte Rufnummer aus. Mit **Zweitwecker Art** wählen Sie, ob der Anruf sofort oder nach der gesamten Rufweiterschaltungszeit beim Teilnehmer signalisiert wird.

9) Klicken Sie auf **OK & Weiter**. Sie befinden sich wieder im Fenster **Rufzielliste - Definition**.

10) Wenn Sie weitere Rufziellisten definieren wollen, wiederholen Sie die vorherigen Schritte.

11) Klicken Sie auf **OK & Weiter**.

12) Ordnen Sie nun den Teilnehmern die Rufziellisten zu.

13) Sie können einen Teilnehmer suchen, indem Sie in die Suchfelder **Rufnr** oder **Name** ein Suchbegriff eingegeben und anschließend die Return-Taste drücken. Alle Treffer werden angezeigt, die den Suchbegriff enthalten. Mit der Eingabe von `521` als Rufnummer werden z. B. die Treffer `+495213535` und `+498967521` angezeigt oder mit `co` als Name die Treffer `Collins`, `Mcoin` und `Branco`.

> ***INFO:*** Alle Einträge werden angezeigt, wenn in allen Suchfeldern nichts eingetragen ist und anschließend die Return-Taste gedrückt wird.

14) Wählen Sie in der Zeile des gewünschten Teilnehmers für die folgenden Fälle aus den Aufklapplisten die Rufziellisten aus:

- **Tag**: Rufzielliste für kommende Externrufe während der Arbeitszeiten (Tagschaltung)
- **Nacht**: Rufzielliste für kommende Externrufe bei aktivierter Nachtschaltung
- **Intern**: Rufzielliste für kommende Internrufe

15) Speichern Sie Ihre Einträge mit **Sichern**, bevor Sie zu einem Teilnehmer auf einer weiteren Seite wechseln.

16) Wenn Sie einer Rufzielliste komfortabel mehrere Teilnehmer zuordnen wollen, klicken Sie auf **Kopieren**.

a) Wählen Sie unter **Rufzielliste** die Rufzielliste aus, der die Teilnehmer zugewiesen werden sollen.

b) Markieren Sie im Fenster **Auswahl** einen oder mehrere Teilnehmer und übernehmen Sie diese mit **Hinzufügen** in das Fenster **Mitglieder**.

c) Wählen Sie über die Kontrollkästchen **Tag**, **Nacht** und **Intern** aus, ob die Rufzielliste für kommende Externrufe während der Arbeitszeiten (Tagschaltung), bei aktivierter Nachtschaltung oder nur für interne Anrufe gelten soll.

d) Klicken Sie auf **OK & Weiter**.

17) Klicken Sie erneut auf **OK & Weiter**.

18) Sie können sich hier alle Teilnehmer einer Rufzielliste anzeigen lassen. Wählen Sie dazu in **Alle Teilnehmer in Rufzielliste anzeigen** die gewünschte Rufzielliste aus.

19) Klicken Sie auf **OK & Weiter**. Die Rufweiterschaltung für interne Teilnehmer ist eingerichtet.

20) Klicken Sie auf **Beenden**.

13.4.2 Anrufumleitung (AUL)

Mit Anrufumleitung (AUL) können Teilnehmer ankommende Anrufe zu einem Ziel Ihrer Wahl umleiten.

Falls Leitungstasten (auch MULAP-Leitungstasten) vorhanden sind, kann die Anrufumleitung auch individuell für eine bestimmte Leitung (oder MULAP-Leitung) aktiviert werden.

Folgende Anrufe können umgeleitet werden:

- Alle Anrufe
- Nur externe Anrufe
- Nur interne Anrufe

Folgende Ziele für eine Anrufumleitung sind möglich:

- Anderes Telefon (intern oder extern)
- Vermittlungsplatz
- Sprachbox
- Sammelanschluss
- UCD-Gruppe (UCD Universelle Anrufverteilung)

Abgehende Anrufe sind bei aktivierter Anrufumleitung weiterhin möglich.

Externes Ziel

Bei einem externen Anrufumleitungsziel geben sie die Amtskennzahl gefolgt von der externen Rufnummer des Umleitungsziels ein.

Anrufumleitung zu externen Zielen

Hat ein Teilnehmer in seiner Rufzielliste eine Anrufumleitung zu einem externen Ziel eingetragen, so endet die Rufweiterschaltung bei diesem Ziel. Eventuell eingetragenen weiteren Ziele in der Rufzielliste wird nicht gefolgt.

Soll eine Rufweiterschaltung zu weiteren Zielen erfolgen, muss das Systemflag **Rufweiterschaltung nach AUL zum externen Ziel** durch einen Servicetechniker aktiviert werden.

Soll einer Anrufumleitung zu einem externen Ziel auch bei einem Anruf über eine analoge Amtsleitung gefolgt werden, muss ein Servicetechniker das Systemflag **Anrufumleitung nach HKZ erlaubt** aktiveren.

Abhängigkeiten

Thema	Abhängigkeit
Anrufschutz	Zu einem anrufgeschützten Telefon können Sie keine Anrufumleitung programmieren.
Termin, Weckeinrichtung	Wird ein Termin fällig, wird dieser Termin am umgeleiteten Telefon signalisiert und nicht von einer eingestellten Umleitung beeinflusst.
UCD-Gruppe als Anrufumleitungsziel	In folgenden Fällen wird der Anrufumleitung zu einer UCD-Gruppe nicht gefolgt: • Wird ein Sammelanschluss gerufen und ein Teilnehmer mit einer Anrufumleitung zu einer UCD-Gruppe ist an der Reihe, wird nicht der Anrufumleitung gefolgt. In diesem Fall wird direkt der nächste Teilnehmer des Sammelanschlusses gerufen. • Ein Teilnehmer ist Mitglied eines Gruppenrufs mit der Eigenschaft “Gruppe” und hat eine Anrufumleitung zu einer UCD-Gruppe aktiviert. • Ein Teilnehmer ist Mitglied eines Gruppenrufs im Freifall. Wird die Gruppe gerufen, wird nicht der Anrufumleitung zur UCD-Gruppe gefolgt. Ausnahme: Der erste eingetragene Teilnehmer hat eine Anrufumleitung zu einer UCD-Gruppe aktiviert. Dieser Anrufumleitung wird gefolgt.

13.4.2.1 Wie Sie Anrufumleitung über analoge Amtsleitungen aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Navigieren Sie im Menübaum zu **System > System Flags**.

4) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie Anrufumleitung über analoge Amtsleitungen aktivieren möchten, aktivieren Sie das Kontrollkästchen **Anrufumleitung nach HKZ erlaubt**.
- Wenn Sie Anrufumleitung über analoge Amtsleitungen deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Anrufumleitung nach HKZ erlaubt**.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

13.4.2.2 Wie Sie eine Anrufumleitung nach Anrufumleitung zum externernen Ziel aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Navigieren Sie im Menübaum zu **System > System Flags**.

4) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie die Anrufumleitung nach Anrufumleitung zum externen Ziel aktivieren möchten, aktivieren Sie das Kontrollkästchen **Rufweiterschaltung nach AUL zum externen Ziel**.
- Wenn Sie die Anrufumleitung nach Anrufumleitung zum externen Ziel deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Rufweiterschaltung nach AUL zum externen Ziel**.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

13.4.3 Anrufumleitung nach Zeit

Die Anrufumleitung nach Zeit leitet nicht angenommene Anrufe nach einer bestimmten Zeit um. Die Anrufumleitung nach Zeit entspricht einer Rufweiterschaltung nach Zeit, nur dass der Teilnehmer die Umleitung selber einstellen kann.

Der Teilnehmer kann die Anrufumleitung nach Zeit für sein eigenes Telefon einstellen, es können auch externe Ziele und Gruppen eintragen werden.

Das Umleitungsziel wird nicht dauerhaft gespeichert und bei Deaktivierung des Leistungsmerkmals gelöscht.

Im Besetztfall gelten die Regeln der Rufweiterschaltung, d. h. es wird mit dem nächsten Ziel fortgefahren.

Systemspezifische Informationen

Pro Teilnehmer gibt es drei einstellbare Ziele. Außerdem gibt es eine Sonderkennung "Benutzerdefiniert", über die der Administrator das Leistungsmerkmal Anrufumleitung nach Zeit für einen Teilnehmer freigeben oder sperren kann. Standardmäßig ist das Leistungsmerkmal freigegeben.

Wird ein Anruf nach der voreingestellten Zeit nicht beantwortet, wird das vom Teilnehmer gespeicherte Umleitungsziel gesucht und gerufen. Ist vom Teilnehmer kein individuelles Umleitungsziel eingetragen, wird mit dem nächsten Ziel in der Rufzielliste fortgefahren.

Der Administrator muss die Anrufumleitung nach Zeit für den einzelnen Teilnehmer über die Rufziellisten freigeben.

13.4.4 Rufweiterschaltung im Amt (nicht für USA)

Jeder Teilnehmer, dem als Durchwahlrufnummer eine MSN (Multiple Subscriber Number beim ISDN-Mehrgeräteanschluss) zugeordnet ist, kann für diese MSN eine Rufweiterschaltung im Amt aktivieren bzw. deaktivieren. Voraussetzung ist, dass der Teilnehmer die Berechtigung für externe Rufweiterschaltung hat.

Ist einer Teilnehmergruppe eine MSN zugeordnet, kann jeder Teilnehmer dieser Gruppe für diese MSN eine Rufweiterschaltung im Amt aktivieren bzw. deaktivieren.

Pro MSN kann nur ein Weiterschaltungsziel eingegeben werden. Die maximale Anzahl weiterschaltbarer MSN ist 10.

Das Leistungsmerkmal wird in drei Varianten unterschieden:

- Unbedingte, sofortige Rufweiterschaltung (CFU Call Forwarding Unconditional) Der Netzanbieter leitet alle für diese MSN bestimmten Rufe direkt weiter, unabhängig von deren Status.
- Rufweiterschaltung im Besetztfall (CFB Call Forwarding Busy) Die Rufweiterschaltung wird nur ausgeführt, wenn die gewählte MSN besetzt ist.
- Rufweiterschaltung im Freifall (CFNR Call Forwarding No Reply) Die Rufweiterschaltung wird nur ausgeführt, wenn der eingehende Ruf nicht innerhalb einer vorgegebenen Zeit beantwortet wird.

Abhängigkeiten

Thema	Abhängigkeit
Nachtschaltung	Rufweiterschaltung im Amt hat höhere Priorität als Nachtschaltung.

13.4.5 Rufzuordnung

Die Rufzuordnung ermöglicht eine Rufweiterschaltung von ankommenden Anrufen einer analogen oder S_0-Leitung zu einem Teilnehmer oder einer Gruppe, abhängig von der gewählten Rufnummer und dem Aktivierungszustand der Nachtschaltung.

Für Tag- und Nachtbetrieb sind unterschiedliche Ziele möglich. Ein ankommender Anruf wird nicht beim Teilnehmer signalisiert, sondern gemäß den Rufziellisten für den Teilnehmer.

13.4.5.1 Wie Sie eine Rufzuordnung konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Leitungen/Vernetzung**.

3) Klicken Sie im Menübaum auf **Leitungen/Vernetzung > Leitungen**.

4) Navigieren Sie im Menübaum unter **Leitungen > …** (Box-Port-Kennzahl) zur gewünschten analogen oder S_0-Leitung.

5) Wählen Sie in der Aufklappliste **Tag Ruf-Nr.** die gewünschte Rufnummer.

6) Wählen Sie in der Aufklappliste **Nacht Ruf-Nr.** die gewünschte Rufnummer.

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

13.4.6 Rufzuschaltung

Das Leistungsmerkmal Rufzuschaltung ermöglicht jedem internen Teilnehmer eine persönliche Liste interner Rufnummern zu verwalten, welche bei Anrufen an seiner Rufnummer ebenfalls gerufen werden.

Ein Teilnehmer kann auch die eigene Rufnummer eintragen, z. B. wenn die Rufnummer fest auf einen anderen Teilnehmer umgeleitet wird (Chef-Sek.).

Zur Aktivierung/Deaktivierung dieses Leistungsmerkmals kann an IP-Systemtelefonen, OpenStage TDM-Telefonen, optiPoint 500-Telefonen eine Taste programmiert werden. Um Variationen zu ermöglichen können auf einem Telefon mehrere Rufzuschaltungstasten programmiert werden. Es können mehrere Tasten gleichzeitig aktiviert werden, allerdings kann die maximale Anzahl Telefone mit Rufsignalisierung fünf nicht überschreiten.

Dieses Leistungsmerkmal kann durch den Teilnehmer für das eigene Telefon über eine DISA-Verbindung oder für einen anderen Teilnehmer mit Hilfe des Leistungsmerkmals Assoziierte Dienste aktiviert/deaktiviert werden.

Die Bildschirmanzeige Weiterleitung ... ist eine von drei Anzeigen im Menü Systemweit von Manager E, die endgerätespezifische (nicht systemspezifische) Statusinformationen liefert. Mit Hilfe des Fensters Weiterleitung können Sie feststellen, ob bei einem Telefon die Rufzuschaltung aktiviert ist oder ob das Telefon Teil einer Rufgruppe ist.

Wird das Leistungsmerkmal häufig benutzt, kann der Teilnehmer eine freie Taste auf seinem Telefon damit belegen. Der Name der Taste ist Rufzuschaltung ein in der Tastenprogrammierung. Bei aktivem Leistungsmerkmal leuchtet die LED.

Durch das Teilnehmer-Flag “keine Rufzuschaltung bei besetzt" kann gesteuert werden, welche rufzugeschalteten Teilnehmer bei besetztem “Master" (= rufzu-

schaltender Teilnehmer) gerufen werden sollen und welche nicht. Haben mehrere “Master" den selben Teilnehmer zugeschaltet, gilt das Flag für alle Zuschaltungen dieses Teilnehmers.

Bei nicht gesetztem Flag wird die Rufzuschaltung auf jeden Fall durchgeführt, sofern der zugeschaltete Teilnehmer erreichbar ist (Standardverhalten).

Bei gesetztem Flag hängt die Rufzuschaltung von der Erreichbarkeit des “Masters" ab:

- “Master" ist frei - Rufzuschaltung erfolgt sofort.
  Beim “Master" kann angeklopft werden - Rufzuschaltung erfolgt nach 5 s.
  Beim “Master" kann nicht angerufen oder angeklopft werden - es erfolgt keine Rufzuschaltung.

Thema	Abhängigkeit/Einschränkung
Wiederanruf Systemsuchlauf Rückruf	Bei einem sofortigen Wiederanruf (z. B. Fehlbedienung) Systemsuchlauf oder Rückruf wird die Rufzuschaltung nicht ausgeführt.
Anrufumleitung	Hat der Teilnehmer, der die Rufzuschaltung aktiviert hat, AUL eingeschaltet, so erfolgt keine Rufzuschaltung.
Anrufschutz (DND)	Hat der rufzugeschaltete Teilnehmer Anrufschutz aktiviert, wird er nicht mitgerufen.
Termin	Ein aktiver Terminruf folgt nicht der Rufzuschaltung.
keine Rufzuschaltung bei besetzt	Ist das Flag gesetzt, wird die Rufzuschaltung nicht ausgeführt, wenn der Teilnehmer besetzt ist.

13.4.7 Abweisen von Anrufen

Ankommende interne und externe Erstanrufe kann der Teilnehmer abweisen. Die Anrufe können durch Betätigen der Trenntaste abgewiesen werden.

Der abgewiesene Anruf folgt anschließend der Rufweiterschaltung. Ist kein Rufweiterschaltungsziel vorhanden, wird ein externer Anruf zum Vermittlungsplatz abgeworfen, sofern die entsprechenden Abwurfkriterien konfiguriert wurden. Wenn kein Ziel gerufen werden kann, dann erhält der Rufende besetzt.

Vermittelte Wiederanrufe, vorgemerkte Rückrufe, gehaltene oder geparkte Gespräche können nicht abgewiesen werden. Wird ein Gespräch zum Abwurfplatz abgeworfen, so kann dieses nicht abgewiesen werden.

Abhängigkeiten

Thema	Abhängigkeit
Gruppenruf, Sammelruf, MULAP	In diesen Fällen wird der gesamte Gruppenanruf beendet und der Anruf folgt der konfigurierten Rufweiterschaltung. Der Anruf wird beendet, falls kein weiteres Rufziel vorhanden ist.

13.4.8 Zurückstellen eines Anrufs

Ein Teilnehmer hat die Möglichkeit einen kommenden Ruf zurückzustellen. Der angerufene Teilnehmer kann eine Verbindung aufbauen, ohne den kommenden Ruf anzunehmen.

Der wartende Ruf wird anschließend als Anklopfen signalisiert.

Wenn ein kommender Ruf signalisiert wird, betätigt der Teilnehmer eine Gesprächs- oder Leitungstaste und tätigt einen externen Anruf. Dafür müssen zwei Gesprächs- und eine Leitungstaste programmiert sein. Eine der entsprechenden Tasten muss für die Ausführung des Leistungsmerkmals frei sein.

Der rufende Teilnehmer bemerkt keinerlei Änderung bei der Signalisierung, wenn Rufsignalisierung bei Anklopfen eingestellt ist.

13.4.9 Anrufschutz

Anrufschutz verhindert die Durchstellung ankommender Anrufe.

Beim Abheben des Hörers erhält der Teilnehmer, der den Anrufschutz aktiviert hat, einen Sonderwählton. Außerdem wird bei Telefonen mit Display Anrufschutz angezeigt, solange das Leistungsmerkmal aktiv ist. Bei allen anderen Telefonen blinkt die LED der Direktruf-Taste des anrufgeschützen Teilnehmers mit einer kleinen Unterbrechung.

Ein gesetzter Anrufschutz kann durch den Vermittlungsplatz oder einen berechtigten Teilnehmer durchbrochen werden. Das Gespräch kann dann auch bei einem Teilnehmer mit Anrufschutz sofort durchgeschaltet werden.

Bei Anwahl eines anrufgeschützten Telefons erhält der Anrufer Besetztton.

Abhängigkeiten

Thema	Abhängigkeit
Vermittlungsplatz/Nachtziel	Der Vermittlungsplatz und der aktuelle Abwurfplatz kann keinen Anrufschutz aktivieren.
Anrufumleitung	Anrufschutz kann nicht aktiviert werden, wenn eine Anrufumleitung auf diesem Telefon aktiviert ist. Auf einem anrufgeschütztes Telefon kann keine Anrufumleitung aktiviert werden.

Thema	Abhängigkeit
Rückruf	Wird ein Rückruf auf einen anrufgeschützten Teilnehmer gesetzt, so wird dieser erst ausgeführt, wenn der Anrufschutz deaktiviert wird. Wenn der anrufgeschützte Teilnehmer einen Rückruf einleitet, wird sein Anrufschutz durchbrochen.
Termin, Weckeinrichtung	Hat ein Teilnehmer einen Termin gesetzt und aktiviert Anrufschutz, erfolgt bei Fälligkeit des Termins eine akustische Signalisierung am Telefon.
DISA	DISA kann vom Anwender für eigene Telefone oder von einem Anwender für einen anderen aktiviert werden (assoziierte Dienste).

13.5 Optimieren der Kommunikationsabläufe

Das Kommunikationssystem bietet verschiedene Möglichkeiten Anrufe komfortabler und effektiver zu handhaben, z. B. Rückruf oder Anklopfen.

13.5.1 Rückruf

Ein Rückruf kann dann aktiviert werden, wenn sich der angerufene Teilnehmer nicht meldet oder besetzt ist. Ein aktivierter Rückruf löst einen Anruf aus, sobald der angerufene Teilnehmer wieder erreichbar ist.

Automatischer Rückruf bei “Frei” oder “Besetzt”

Wenn ein Gesprächswunsch nicht erfüllt wird, weil der gerufene Teilnehmer besetzt ist oder den Anruf nicht annnimmt, kann der rufende Teilnehmer einen Rückruf aktivieren, um das Gespräch zu einem späteren Zeitpunkt aufzubauen. War der gerufene Teilnehmer besetzt, wird durch Rückruf das Ende des Gesprächs überwacht. Wenn der Teilnehmer wieder frei ist, wird dies dem rufenden Teilnehmer signalisiert, indem er selbst nun durch das Kommunikationssystem angerufen wird. Nimmt er diesen Anruf an, wird der zuvor besetzte Teilnehmer erneut angewählt. Bei Nichtzustandekommen eines Gesprächs durch die Rückruffunktion, bleibt diese aktiv. Sobald der gewünschte Teilnehmer ein neues Gespräch geführt hat, erfolgt erneut ein Rückruf.

Ein Telefon kann bis zu zwei Rückrufanforderungen abschicken und Ziel von bis zu zwei Anforderungen sein. Mehr gehende Anforderungen werden abgewiesen.

Rückrufanforderungen werden gelöscht wenn

- das Gespräch zustande gekommen ist, wenn nicht, bleibt der Rückruf weiter aktiv (bei einem internen Rückruf),
- der Rückruf aufgebaut wurde ohne dass ein Gespräch zustande gekommen ist (bei einem externen Rückruf),
- der einleitende Teilnehmer den Rückruf löscht,

- das System täglich um 23:57 Uhr alle Rückrufe löscht.

Rückrufanforderungen können auf interne Teilnehmer und Gruppen gesetzt werden. Bei einem Gruppenanschluss wird eine Rückrufaufforderung beim ersten Teilnehmer hinterlegt. Bei einem Rückruf auf einen Gruppenanschluss klingeln alle Telefone, die frei sind.

Automatischer Rückruf bei frei auf der Amtsschnittstelle

Ein interner Teilnehmer, der einen externen freien Teilnehmer nicht erreicht, kann einen Rückrufwunsch im Amt aktivieren. Daraufhin wird der Anschluss des angerufenen Teilnehmers überwacht. Sobald der angerufene Teilnehmer selbst einen Verbindungsaufbau einleitet und diese Verbindung wieder beendet, wird vom Amt versucht eine Verbindung zwischen den beiden Teilnehmern herzustellen. Dieses Leistungsmerkmal muss vom Amt unterstützt werden.

Rückruf bei Besetzt

Auf eine externe, besetzte Nebenstelle kann ein manueller Rückruf gesetzt werden. Nach Freiwerden des Teilnehmers wird vom Amt versucht, eine Verbindung zwischen den beiden Teilnehmern herzustellen. Das Leistungsmerkmal muss vom Amt und der Gegenstelle unterstützt und freigeschalten sein.

13.5.2 Anklopfen

Anklopfen signalisiert einem Teilnehmer im Gespräch einen weiteren ankommenden Anruf.

Die Signalisierung wird optisch durch eine Nachricht im Display angezeigt. Die Signalisierung kann auch akustisch durch einen kurzen Anklopfton erfolgen. Der Anklopfton ist alle 5 Sekunden hörbar.

Der gerufene Teilnehmer hat die Möglichkeit, dieses zweite Gespräch anzunehmen oder zu ignorieren. Um den zweiten Anruf anzunehmen, kann der Teilnehmer die erste Verbindung beenden und das zweite Gespräch annehmen oder die im Display angebotene Funktion **Anklopfen annehmen** auswählen. In diesem Fall wird das erste Gespräch gehalten.

Bei einem Teilnehmer kann nicht angeklopft werden, wenn bereits bei diesem Teilnehmer jemand anklopft (max. 4 Teilnehmer können anklopfen) oder dieser Anklopfschutz aktiviert hat. Es erfolgt Besetztsignalisierung zum Anrufer, wenn keine Rufweiterschaltung im Besetztfall konfiguriert ist.

Anklopfen freigeben

Das Flag **Anklopfschutz** muss für den Teilnehmer gesetzt sein, damit dieser Teilnehmer zwischen Anklopfen freigeben und Anklopfen unterdrücken über Menü oder Kennzahl wählen kann. Hat ein Teilnehmer Anklopfen freigegeben, wird bei Ihm auch dann angeklopft, wenn er Rufweiterschaltung im Besetztfall konfiguriert hat.

Anklopfen durch den Vermittlungsplatz

Die Standardeinstellung ist immer Anklopfen nach Zeit. Der Vermittlungsplatz kann aber auch sofort Anklopfen.

Abhängigkeiten

Thema	Abhängigkeit
Stilles Anklopfen	Der Anklopfton kann durch den Teilnehmer mit einer Kennzahl aktiviert/deaktiviert werden. Die optische Signalisierung des Anklopfens im Display des Telefons bleibt erhalten. Standard ist Anklopfton ein.
Aufschalten	Ist Anklopfschutz aktiviert, wird verhindert, dass ein Aufschalten auf eine Verbindung dieses Teilnehmers erfolgen kann.
Gruppenruf	Wenn ein oder mehrere Teilnehmer eines Gruppenrufes frei sind, wird ihnen der Anruf angeboten. Sind alle Teilnehmer besetzt, bekommen alle eine Anklopfsignalisierung, außer alle Teilnehmer haben Anklopfschutz aktiviert.
Direktansprechen	Direktansprechen zu besetzten Teilnehmern ist nicht möglich.

13.5.2.1 Wie Sie Anklopfen aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Teilnehmer**.

3) Klicken Sie im Menübaum auf **Teilnehmer**.

4) Klicken Sie z. B. auf **IP Clients**.

5) Klicken Sie z. B. auf **SystemClients**.

6) Wählen Sie den entsprechenden Teilnehmer aus.

7) Klicken Sie auf die Registerkarte **Teilnehmer-Flags ändern**.

8) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie Anklopfen aktivieren möchten, deaktivieren Sie das Kontrollkästchen **Anklopfschutz ein**.
- Wenn Sie Anklopfen deaktivieren möchten, aktivieren Sie das Kontrollkästchen **Anklopfschutz ein**.

9) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

13.5.2.2 Wie Sie sofortiges Anklopfen durch Vermittlungsplatz aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **System**.

4) Klicken Sie auf **Abwurf/VPL/Hotline**.

5) Wählen Sie eine der folgenden Möglichkeiten unter **Sonstige Kriterien**:

- Wenn Sie die Funktion aktivieren möchten, aktivieren Sie das Kontrollkästchen **Sofortiges Anklopfen durch VPL**.
- Wenn Sie die Funktion deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Sofortiges Anklopfen durch VPL**.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

13.5.3 Aufschalten

Mit Aufschalten kann ein berechtigter Teilnehmer sich in ein Gespräch eines internen Teilnehmers einschalten.

Das Aufschalten erfolgt mittels Kennziffer oder Taste und wird den beteiligten Teilnehmern durch einen Aufmerksamkeitston und durch die Anzeige im Display mitgeteilt.

Dieses Leistungsmerkmal kann während des Besetztsignals oder während des Anklopfens aktiviert werden.

Beim Aufschalten auf eine Verbindung gilt Folgendes:

- Wenn der gerufene Teilnehmer auflegt, bekommt er einen Anruf vom vermittelnden Teilnehmer.
- Wenn der aufschaltende Teilnehmer (der das Gespräch vermitteln möchte und sich aufschaltet) auflegt, wird das Gespräch zum Zielteilnehmer vermittelt.
- Wenn der Teilnehmer, der mit dem gerufenen Teilnehmer verbunden wurde, auflegt, bleiben der aufgeschaltete und der gerufene Teilnehmer verbunden.

Aufschalten kann jeder interne Teilnehmer und der Abwurfplatz (Vermittlungsplatz). Um dieses Leistungsmerkmal nutzen zu können, muss der interne Teilnehmer und auch der Abwurfplatz dafür berechtigt werden.

Es ist nicht möglich das Aufschalten auf ein bestimmtes Telefon zu verhindern.

Abhängigkeiten

Thema	Abhängigkeit
Sprachkanal-Signalisierungsschutz	Ist der angerufene Teilnehmer oder dessen interner Gesprächspartner als Datenstation eingetragen (Sprachkanal-Signalisierungsschutz) oder ist der angerufene Teilnehmer im Wahlzustand, kann nicht aufgeschaltet werden.
Anrufschutz	Wenn der gerufene Teilnehmer den Anrufschutz aktiviert hat, kann nur ein Gespräch aufgeschaltet werden, wenn der Teilnehmer ein Gespräch führt.
Gruppe/Sammelanschluss	Sind beim Rufen einer Gruppe oder eines Sammelanschlusses alle Teilnehmer besetzt, ist kein Aufschalten möglich.
S_0-Teilnehmer	Das Aufschalten auf einen S_0-Teilnehmer ist nicht möglich.

13.5.3.1 Wie Sie einen internen Teilnehmer für das Aufschalten berechtigen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Teilnehmer**.

3) Klicken Sie im Menübaum auf **Teilnehmer**.

4) Klicken Sie im Menübaum auf den Teilnehmer (Index - Rufnummer - Name).

5) Klicken Sie auf die Registerkarte **Teilnehmer-Flags ändern**.

6) Aktivieren Sie das Kontrollkästchen **Aufschalteberechtigung ein**.

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

13.5.3.2 Wie Sie den Abwurfplatz für das Aufschalten berechtigen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **System > Abwurf/VPL/Hotline**.

4) Aktivieren Sie im Bereich **Sonstige Kriterien** das Kontrollkästchen **Überschreiben durch VPL**.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

13.5.4 Abwesenheitstexte

Der Abwesenheitstext eines Teilnehmers erscheint im Display des Anrufers.

In Abwesenheitstexten (auch als Antwort-Text bezeichnet) können variable Parameter vergeben werden. Diese Parameter (z. B. Uhrzeit) werden während der Aktivierung eingegeben. Für die Eingabe der ergänzenden Zeichen steht der Ziffernblock des Endgerätes zur Verfügung. Der Abwesenheitstext kann über eine Kennzahl oder über eine zuvor eingerichtete Funktionstaste an einem Telefon aktiviert/deaktiviert werden.

Anrufumleitung

Bei Anrufumleitung wird der Abwesenheitstext des angerufenen Teilnehmers angezeigt und der Anrufumleitung gefolgt.

13.5.4.1 Wie Sie einen Abwesenheitstext ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **System**.

4) Klicken Sie auf **Texts**.

5) Klicken Sie in der Spalte **Antwort-Texte** in das entsprechende Feld und geben Sie den Abwesenheitstext ein.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

13.5.5 Mitteilungstexte

Mitteilungstexte sind systeminterne Texte, die ein Teilnehmer auswählen und an interne Teilnehmer senden kann.

Ein Mitteilungstext (Info-Text) kann an einen oder mehrere Empfänger gesendet werden.

Soll der Text an alle Mitglieder einer internen Gruppe oder eines internen Sammelanschlusses verschickt werden, muss man die Rufnummer der Gruppe

oder des Sammelanschlusses anstelle eines einzelnen Teilnehmers als Empfänger angeben.

Das Versenden erfolgt mittels Taste oder Menü Info senden.

Das Senden kann im Ruhe-, Ruf-, Gesprächs- oder Besetztzustand erfolgen. Im Rufzustand entfällt die Angabe der Rufnummer des Empfängers.

13.5.5.1 Wie Sie einen Mitteilungstext ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **System**.

4) Klicken Sie auf **Texts**.

5) Klicken Sie in der Spalte **Info-Texte** in das entsprechende Feld und geben Sie den Text ein.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

13.5.6 Assoziierte Dienste

Ein berechtigter Teilnehmer kann für einen beliebigen anderen Teilnehmer Leistungsmerkmale stellvertretend steuern, z. B. Anrufumleitung, Codeschloss oder Sammelanschluss ein / aus. Die Auswirkung ist die gleiche, wie bei der Aktivierung oder Deaktivierung jenes Leistungsmerkmals durch den anderen Teilnehmer für sich selbst.

Folgende Leistungsmerkmale sind stellvertretend steuerbar:

- Anrufumleitung ein / aus
- Codeschloss ein / aus
- Rufzuschaltung ein / aus
- Antworttext ein / aus
- Sammelanschluss und Gruppenruf ein / aus
- Nachtschaltung ein / aus
- Termin ein / aus
- Info senden / gesendete Infos löschen
- Codeschloss Kennwort ändern
- UCD-Agent einloggen / ausloggen
- UCD-Agent verfügbar / nicht verfügbar
- UCD-Agent Nachbearbeitung ein / aus

- UCD-Agent Nachtschaltung ein / aus
- Umleitung MULAP ein / aus
- Aktivierte Leistungsmerkmale zurücksetzen

Die Nutzung erfolgt mittels einer Prozedur. Der Teilnehmer muss Folgendes angeben:

- Die Kennzahl für Assoziierte Dienste
- Die Rufnummer des Teilnehmers, für den eine Aktion ausgeführt werden soll
- Die Kennzahl des zu steuernden Leistungsmerkmales

Bevor ein Teilnehmer Assoziierte Dienste benutzen kann, muss er das Codeschloss des anderen Teilnehmers deaktivieren, falls aktiviert.

13.5.6.1 Wie Sie Assoziierte Dienste aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Teilnehmer**.

3) Klicken Sie im Menübaum auf **Teilnehmer**.

4) Klicken Sie im Menübaum auf den Teilnehmer (Index - Rufnummer - Name).

5) Klicken Sie auf die Registerkarte **Teilnehmer-Flags ändern**.

6) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie die Funktion aktivieren möchten, aktivieren Sie das Kontrollkästchen **Assoziierte Wahl/Dienste**.
- Wenn Sie die Funktion deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Assoziierte Wahl/Dienste**.

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

13.5.7 DISA

DISA (Direct Inward System Access) ermöglicht berechtigten Teilnehmern die Nutzung von Leistungsmerkmalen des Kommunikationssystems von außerhalb, z. B. am Mobiltelefon über myPortal for Mobile (bei Mobile Callback) und Mobility.

Ein Teilnehmer kann über DISA auch gehende Verbindungen aufbauen, sowohl intern als auch extern. Der Teilnehmer muss bei jeder Benutzung von DISA das Passwort für das Codeschloss eingeben. Anschließend stehen bestimmte Leistungsmerkmale zur Verfügung wie bei interner Nutzung.

DISA unterstützt folgende Leistungsmerkmale:

Leistungsmerkmal	durch den Teilnehmer selbst	über Assoziierte Dienste
Anrufumleitung ein / aus	x	x
Anrufschutz ein / aus	x	x
Sammelanschluss ein / aus	x	x
Abwesenheitstext ein / aus	x	x
Rufzuschaltung ein / aus	x	x
Codeschloss ein / aus	x	x
Dienste zurücksetzen	x	x
Kurzwahl zentral (KWZ)	x	–
Infotext senden	x	–
Nachtschaltung ein / aus	x	–

Der Administrator legt fest, unter welcher Rufnummer die Teilnehmer DISA nutzen können. Die Rufnummer kann für externe und interne Nutzung unterschiedlich sein. Intern bedeutet an einem anderen mittels IP-vernetzten Knoten.

Das vom Teilnehmer einzugebende Passwort besteht aus der internen Rufnummer und der PIN für das Codeschloss. Nach der Eingabe des Passworts muss der Teilnehmer entweder die Taste # drücken oder warten, bis das Kommunikationssystem seine Eingabe erkannt hat, je nach dem vom Administrator festgelegten Sicherheitsmodus für DISA.

Für eine weitere Aktion über DISA muss sich der Teilnehmer erneut anmelden.

13.5.7.1 Wie Sie die DISA-Berechtigung für einen Teilnehmer aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Teilnehmer**.

3) Klicken Sie im Menübaum auf **Teilnehmer**.

4) Klicken Sie im Menübaum auf den Teilnehmer (Index - Rufnummer - Name).

5) Klicken Sie auf die Registerkarte **Teilnehmer-Flags ändern**.

6) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie die Funktion aktivieren möchten, aktivieren Sie das Kontrollkästchen **DISA Berechtigung**.

- Wenn Sie die Funktion deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **DISA Berechtigung**.

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

13.5.7.2 Wie Sie eine DISA-Nummer konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **Grundeinstellungen > System > DISA**.

4) Geben Sie im Feld **Durchwahl** die Rufnummer ein, über welche die Teilnehmer DISA von extern nutzen können.

5) Geben Sie im Feld **Rufnummer** die Rufnummer ein, über welche die Teilnehmer DISA von intern nutzen können.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

13.5.7.3 Wie Sie den DISA-Sicherheitsmodus konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **Grundeinstellungen > System > DISA**.

4) Wählen Sie in der Aufklappliste **Sicherheits-Modus** den Sicherheitsmodus **Nach Zeit** oder **Nach Eingabe #**.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

13.5.8 Flex Call/Mobile PIN

Mit Flex Call (Mobile PIN) wird ein Systemtelefon für das nächste gehende Gespräch vorübergehend von einem anderen Teilnehmer so genutzt, als wäre es sein eigenes.

Flex Call beinhaltet die Rufnummer, den Namen, die Amtsberechtigung und die Gebührenerfassung dieses Teilnehmers.

Ist Flex Call aktiviert, kann das benutzte Telefon nicht unter seiner eigentlichen Rufnummer erreicht werden. Nach Gesprächsende wird dieser Zustand wieder aufgehoben.

Für die Aktivierung von Flex Call muss ein individuelles Codeschloss für den mobilen Teilnehmer vergeben sein.

Zur Aktivierung ist einer der folgenden Schritte am Systemtelefon durchzuführen:

- OpenStage: Service-Menü > PIN und Berechtigung > Flex Call + mobile Rufnummer + Codeschloss des mobilen Teilnehmers
- Kennzahl für FlexCall + mobile Rufnummer + Codeschloss des mobilen Teilnehmers

13.5.9 Relocate/Rufnummerntausch

Über Relocate/Rufnummerntausch kann ein OpenStage-TDM-Teilnehmer die Zuordnung zwischen physikalischem Anschluss-Port und logischen Teilnehmerdaten (Benutzerprofil) per Prozedur ändern.

Relocate kann angewendet werden, wenn zwei Teilnehmer sich zu einem Tausch ihrer Arbeitsplätze entschließen und beide dieselben Telefontypen benutzen. Relocate ermöglich so die Realisierung von DeskSharing für TDM-Teilnehmer. Die TDM-Teilnehmer können ohne Unterstützung eines Administrators den Rufnummerntausch selbst durchführen.

Es dürfen nur Benutzerprofile des gleichen Telefontyps, d. h. mit identischem Tastenlayout getauscht werden. Beim Tausch von Benutzerprofilen unterschiedlicher Telefontypen werden individuell programmierte Tastenfunktionen des Grundgerätes durch die Default-Werte ersetzt. Bei der Durchführung von Relocate kommt es zu einem Ausfall/Neustart der beteiligten TDM-Telefone. Aktivierte Leistungsmerkmale werden dementsprechend behandelt, d. h. aktuelle Rückrufe und versandte Infos werden gelöscht, alle anderen Leistungsmerkmale bleiben erhalten.

Voraussetzung für die Nutzung von Relocate ist die systemweite Freigabe des Leistungsmerkmals. Für den Rufnummerntausch wählen Sie im Service-Menü des zu tauschenden Telefons Rufnr. tauschen und geben die interne Rufnummer des Zielteilnehmers und die Codeschloss-PIN ein (Codeschloss-PIN ist nicht erforderlich, wenn die PIN dem Default 00000 entspricht). Nach Eingabe der Zielrufnummer ist Relocate bis zum Abschluss der Prozedur für alle anderen Teilnehmer gesperrt. Bei Ausführung des Tausches werden die beiden beteiligten Endgeräte zurückgesetzt. Der erfolgreiche Tausch wird an beiden TDM-Telefonen durch die Anzeige der neuen Rufnummer signalisiert (Display-Anzeige: Neue Rufnr.: XXXXX).

Relocate kann nicht an Systemtelefonen mit Programmierberechtigung (für Assistant T) durchgeführt werden. Also in der Regeln nicht an den ersten zwei aktiven Systemtelefonen.

13.5.9.1 Wie Sie Relocate/Rufnummertausch systemweit freigeben

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Grundeinstellungen > System**.

3) Klicken Sie im Menübaum auf **System Flags**.

4) Aktivieren Sie das Kontrollkästchen **Endgerätetausch erlaubt**.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

13.5.10 Rücksetzen aktivierter Leistungsmerkmale

Sie können an Ihrem Endgerät bestimmte Leistungsmerkmale gemeinsam mittels Kennzahl rücksetzen.

Dies ist möglich für folgende Leistungsmerkmale:

- Anrufumleitung
- Empfangene Infos löschen
- Antworttext ein / aus
- Rufzuschaltung ein / aus
- Sammelanschluss ein / aus
- Rufnummernunterdrückung ein / aus
- Stilles Anklopfen ein / aus
- Anrufschutz ein / aus
- Ruhe ein / aus
- Termin
- Alle Rückrufe löschen

13.5.11 Prozeduren

Das Kommunikationssystem ermöglicht dem Teilnehmer das Speichern von Kennzahlen, Rufnummern sowie weiteren Wahlinformationen als Prozeduren auf einer Taste. Drückt der Teilnehmer die Prozedurtaste in Nachwahl oder während eines Gespräches, sendet das Kommunikationssystem die entsprechenden MFV-Zeichen (MFV = Mehrfrequenzwahlverfahren).

Anwendungsbeispiele:

- Kennzahl für Rückruf
- Kennzahl für Anklopfen

- Kennzahl für Aufschalten
- Ziffernfolge für Sprachbox oder Anrufbeantworter
- Amts-Flashkennzahl + Zielrufnummer
- Kennzahl zur Steuerung eines Dienstes + Zielrufnummer, z. B. Kennzahl für Info (Message Waiting) senden / abfragen + Rufnummer + Textnummer
- PKZ (Projektkennzahl) + Bündelkennzahl + Zielrufnummer

Prozeduren, welche die Eingabe einer PIN erfordern, können nicht gespeichert werden.

Nur die ersten Tastenebene unterstützt Prozedurtasten.

Ein Teilnehmer kann in Prozeduren situationsabhängig folgende Leistungsmerkmale nutzen:

Leistungsmerkmal	wahlbereit	besetzt	im Gespräch	gehender Ruf	kommender Ruf
Anrufübernahme, gezielt	x	–	x	–	–
Anrufumleitung ein (nicht bei Gemeinschaftsanlagen; nicht für einzelne MSN eines S_0-Amtsanschlusses)	x	–	x	x	–
Anrufumleitung im Amt ein / aus; Umschaltfunktion; (nicht bei Gemeinschaftsanlagen);	x	–	x	x	–
Anrufverteilung, Anmelden / Abmelden; Umschaltfunktion	x	–	x	x	–
Anrufverteilung, Nachtziel ein / aus; Umschaltfunktion	x	–	x	x	–
Anrufumleitung pro Teamschaltung	x	x	x	x	x
Antworttext ein / aus; Umschaltfunktion	x	–	x	x	–
Assoziierte Wahl	x	x	x	x	x
Assoziierte Dienste	x	–	x	x	–
Direktansprechen	x	–	x	–	–
Freischalten von Leitungen (Emergency Trunk Access)	x	–	x	x	–
Infos (Message Waiting) senden	x	–	x	x	–
KWI ausspeichen	x	–	x	x	–
KWZ ausspeichen	x	–	x	x	–
MFV-Übertragung	–	–	x	–	–
MFV-Übertragung im Gesprächszustand mittels Prozedurtaste	x	x	x	x	x
Nachtschaltung ein / aus; Umschaltfunktion	x	–	x	x	–
Parken / Wiederaufnehmen; Umschaltfunktion	–	x	x	x	–
Projektkennzahl PKZ	x	–	x	–	–
Projektkennzahl PKZ in Vorwahl	x	–	x	–	–
Rückrufaufträge anzeigen / löschen; Umschaltfunktion	x	–	–	–	–
Rufzuschaltung ein / aus; Umschaltfunktion	x	–	x	x	–

Leistungsmerkmal	wahlbereit	besetzt	im Gespräch	gehender Ruf	kommender Ruf
Sprachauswahl	x	x	x	x	x
Telephone Data Service TDS	x	–	x	x	–
Türöffner via Adapterbox	x	x	x	x	x
Termin ein / aus; Umschaltfunktion	x	x	x	x	x
Wiederaufnahme eines externen Gesprächs aus allgemeinem Halten	x	x	x	x	x
Zentrales Codeschloss	x	–	x	–	–

Systemspezifische Informationen

Eine Prozedurtaste kann maximal 32 Zeichen speichern.

13.5.12 Weckeinrichtung und Termine

Jeder Teilnehmer hat die Möglichkeit, einen Termin zu programmieren. Zum Fälligkeitszeitpunkt erfolgt ein Terminruf. Der Termin kann einmalig (innerhalb der nächsten 24 Stunden) oder wiederholt (d. h. täglich) ausgeführt werden.

Die Eingabe der Terminzeit erfolgt durch vier Ziffern, von denen die ersten zwei die Stunde und die letzten zwei die Minute festlegen. Für die USA wird eine Zeitangabe im 12-Stundenmodus unterstützt, wobei der Teilnehmer nach Eingabe der vier Ziffern noch “am" (= Taste 2) oder "pm" (= Taste 7) nachwählen kann. Bei fehlender Angabe wird "am" angenommen.

Analoge Telefone, optiPoint 500 entry oder CMI-Telefone können nur einmalige Termine programmieren.

Ein Terminruf dauert standardmäßig 20 Sekunden und wird bis zu fünfmal mit einer jeweils einminütigen Pause wiederholt. Das Löschen des Auftrags erfolgt automatisch durch Abnehmen des Handapparates oder Betätigen der Lautsprechertaste während des Rufes oder nach der fünften Wiederholung (Anzahl konfigurierbar). Ein programmierter Terminruf kann alternativ auch mit einer Prozedur gelöscht werden. Bei Display-Endgeräten besteht zudem eine Abfragemöglichkeit.

Kann ein fälliger Terminruf nicht signalisiert werden (z. B. Teilnehmer besetzt), so wird er bis zum nächsten Zyklus zurückgestellt.

14 Arbeiten im Team (Gruppen)

Für das Arbeiten im Team stellt das Kommunikationssystem vielfältige Leistungsmerkmale zur Verfügung. Neben Anrufübernahmegruppen, Gruppenrufen und Sammelanschlüssen gehören dazu auch Gruppen mit Team- und Chef/Sekretär-Funktionen und Sprachbox- und Faxbox-Gruppen. Durch das Leistungsmerkmal "Anrufverteilung (UCD Uniform Call Distribution)" wird eine gleichmäßige Verteilung von eingehenden Anrufen auf eine Gruppe von Teilnehmern (UCD-Gruppe) ermöglicht.

INFO: Bei der Konfiguration von Gruppen ist zu beachten, dass die ersten drei Gruppen reserviert sind:

Die erste Gruppe wird standardmäßig als Sammelanschluss für Xpressions Compact verwendet.

Die zweite Gruppe wird standardmäßig als Sammelanschluss für OpenScape Business Smart VoiceMail verwendet.

Die dritte Gruppe wird standardmäßig als Sammelanschluss für den Company AutoAttendant der OpenScape Business Smart VoiceMail verwendet.

14.1 Anrufübernahmegruppe, Gruppenruf und Sammelanschluss

Das Kommunikationssystem bietet verschiedene Möglichkeiten, um Teilnehmer zu Gruppen zusammenzufassen, damit mehrere Teilnehmer und Telefone zum Beispiel unter einer Rufnummer erreichbar sind oder ein Anruf für einen Teilnehmer auch bei anderen Teilnehmern signalisiert wird.

Bei einer Anrufübernahmegruppe wird der Anruf für ein Mitglied immer auch bei allen anderen Gruppenmitgliedern signalisiert.

Bei einem Gruppenruf sind alle Mitglieder unter einer Rufnummer (Gruppenrufnummer) erreichbar. Der zuerst abhebende Teilnehmer wird mit dem Anrufenden verbunden.

Bei einem Sammelanschluss wird ein ankommender Anruf bei einem der Mitglieder signalisiert. Nimmt dieser den Anruf nicht entgegen, wird das Gespräch dem nächsten Mitglied zugewiesen. Alle Mitglieder des Sammelanschlusses sind unter einer Rufnummer erreichbar.

14.1.1 Anrufübernahmegruppe

Ein Anruf für ein Mitglied einer Anrufübernahmegruppe (AUN-Gruppe) wird auch bei allen anderen Gruppenmitgliedern signalisiert. Der Anruf kann mittels einer dafür programmierten Funktionstaste oder über den zugehörigen Menüeintrag

des Telefons oder durch das Wählen der Kennzahl von allen anderen Gruppenmitgliedern angenommen werden.

Beim ursprünglich gerufenen Mitglied der Anrufübernahmegruppe wird der Anruf akustisch und optisch (Display) signalisiert. Falls programmiert, wird der Anruf auch über die LED der Funktionstaste signalisiert.

Die anderen Gruppenmitglieder erhalten zuerst nur eine optische Signalisierung des Anrufs. Im Display werden Rufnummer oder Name des ursprünglich gerufenen Teilnehmers und Rufnummer oder Name des Anrufers angezeigt. Die Anzeige der Rufnummer oder des Namens des Anrufers kann durch einen Administrator mit dem Profil **Expert** über den **Experten-Modus** deaktiviert werden. Falls programmiert, wird der Anruf auch über die LED der Funktionstaste signalisiert.

Wird der Anruf nicht innerhalb von vier Rufzyklen (4 x 5 Sekunden) angenommen, erhalten die anderen Gruppenmitglieder einen Aufmerksamkeitston (akustische Signalisierung). Die Zeit vom Start der Anrufsignalisierung bis zum Aufmerksamkeitston ist nicht variabel. Der Aufmerksamkeitston kann durch einen Administrator mit dem Profil **Expert** über den **Experten-Modus** für alle Gruppenmitglieder deaktiviert werden.

Bei mehreren Anrufen für eine Anrufübernahmegruppe erfolgt die Signalisierung in der Reihenfolge des Anrufeingangs.

Sollen Wiederanrufe für Mitglieder einer AUN-Gruppe auch durch die anderen Mitglieder übernommen werden können, muss dies durch einen Administrator mit dem Profil **Expert** über den **Experten-Modus** aktiviert werden.

Ein Teilnehmer kann nur Mitglied in einer Anrufübernahmegruppe sein.

Eventuell anfallende Gebühren für einen übernommenen Anruf werden dem Teilnehmer zugewiesen, der den Anruf übernommen hat.

SIP-Telefone

Die Einbindung von SIP-Telefonen in eine Anrufübernahmegruppe ist möglich.

> ***INFO:*** Zusätzlich kann für SIP-Telefone eine Funktionstaste für die Anrufübernahmegruppe programmiert werden und die spezifische Meldungen einer Anrufübernahmegruppe können im Display der SIP-Telefone angezeigt werden. Um dies zu nutzen, muss das Leistungsmerkmal "Anrufübernahmegruppe" am SIP-Telefon aktiviert werden (siehe Bedienungsanleitung des SIP-Telefons).

Anrufübernahme außerhalb einer AUN-Gruppe

Eine Variante des Leistungsmerkmals ist die "Anrufübernahme außerhalb einer AUN-Gruppe". Ermöglicht wird damit die Übernahme von Anrufen für interne Teilnehmer, die nicht zur gleichen AUN-Gruppe gehören. Die Übernahme des Anrufs ist über eine dafür programmierte Funktionstaste oder über den Menüeintrag oder durch das Wählen der Kennzahl für Anrufübernahme gezielt

und die anschließende Eingabe der Rufnummer des gerufenen Teilnehmers möglich.

Abhängigkeiten

Thema	Abhängigkeit
Rückruf	Wiederanrufe und Rückrufe werden bei den anderen Gruppenmitgliedern nur signalisiert, wenn das System-Flag **Anrufübernahme nach Wiederanruf** aktiviert ist.
Anrufschutz	Teilnehmer mit aktiviertem Anrufschutz erhalten keine Anrufübernahme-Signalisierung.
ISDN-Telefone	Die Einbindung von ISDN-Telefonen in Anrufübernahmegruppen ist nicht möglich.
MULAP	Die Einbindung von MULAP-Rufnummern in Anrufübernahmegruppen ist nicht möglich.

Verwandte Themen

- Wie Sie Anrufübernahmegruppen konfigurieren
- Wie Sie ein Mitglied zur Anrufübernahmegruppe hinzufügen oder löschen
- Wie Sie die Anzeige der Rufnummer und des Namens des Anrufers aktivieren oder deaktivieren
- Wie Sie den Aufmerksamkeitston aktivieren oder deaktivieren
- Wie Sie die Anrufübernahme von Wiederanrufen aktivieren oder deaktivieren

14.1.2 Gruppenruf

Sollen mehrere Teilnehmer unter einer Rufnummer (Gruppenrufnummer) erreichbar sein, kann ein Gruppenruf definiert werden. Ankommende externe und interne Anrufe werden gleichzeitig bei allen Gruppenmitgliedern signalisiert. Der zuerst abhebende Teilnehmer wird mit dem Anrufenden verbunden.

Jedes Mitglied eines Gruppenrufs ist auch unter seiner eigenen Teilnehmerrufnummer erreichbar.

Der Gruppe muss eine der folgenden Eigenschaften zugewiesen werden:

- Gruppe
  Ankommende Anrufe werden gleichzeitig bei allen verfügbaren Gruppenmitgliedern signalisiert. Verfügbare Gruppenmitglieder sind Teilnehmer, die nicht besetzt sind. Sind alle Gruppenmitglieder besetzt, wird ein Anruf durch einen Anklopfton signalisiert. Legt ein Teilnehmer auf, wird der Anruf weiterhin bei allen Gruppenmitgliedern signalisiert (Anklopfton bei besetzten Gruppenmitgliedern).
  Sind alle Gruppenmitglieder besetzt und alle haben das Leistungsmerkmal "Anklopfschutz" aktiviert, erhält ein Anrufer den Besetztton. Ist ein Rufweiterschaltungsziel für diese Gruppe definiert, erhält der Anrufer keinen

Besetztton, sondern wird direkt zum nächsten Rufweiterschaltungsziel geleitet.

- Freifall
  Ankommende Anrufe werden gleichzeitig bei allen Gruppenmitgliedern signalisiert. Ist ein Mitglied der Gruppe besetzt, wird der gesamte Gruppenruf als besetzt gekennzeichnet. Weitere Anrufer erhalten den Besetztton.
- Anklopfen
  Ankommende Anrufe werden gleichzeitig bei allen verfügbaren Gruppenmitgliedern signalisiert. Verfügbare Gruppenmitglieder sind Teilnehmer, die nicht besetzt sind. Bei besetzten Gruppenmitgliedern wird ein anstehender Anruf sofort durch einen Anklopfton signalisiert.
  Voraussetzung dafür ist, dass bei allen Gruppenmitgliedern der Anklopfschutz deaktiviert wird.

Gruppenrufe werden von der Rufweiterschaltung wie Teilnehmer behandelt. Das heißt, wenn ein Anruf von keinem Mitglied eines Gruppenrufs angenommen werden kann, wird dieser zu einem Rufweiterschaltungsziel entsprechend der Rufzielliste weitergeschaltet. Dabei kann unterschieden werden, ob eine Rufweiterschaltung im Freifall oder im Freifall und Besetztfall erfolgen soll.

Wenn ein Anruf von keinem Mitglied eines Gruppenrufs angenommen wurde, wird dieser als entgangener Anruf im Journal der UC Clients aller Mitglieder angezeigt. Ein angenommener Anruf wird nur im Journal des Mitglieds angezeigt, der den Anruf angenommen hat.

Ein einzelner Teilnehmer kann gleichzeitig mehreren Gruppen angehören. Für die Gruppen des Typs Gruppenruf, Sammelanschluss, Teamschaltung/Team-Gruppe und Chef/Sekretär/Top-Gruppe gilt: Die Summe aller Mitgliedschaften des Teilnehmers in diesen Gruppen darf 32 nicht übersteigen.

Im Display eines rufenden internen Teilnehmers wird der zugewiesene Gruppenname angezeigt. Nach Annahme eines Anrufs, wird der Name des Teilnehmers angezeigt, der den Anruf angenommen hat.

Hat ein Mitglied über den AutoAttendant Regeln definiert, zum Beispiel für die Weiterschaltung von Anrufen, gelten diese nur für Anrufe an seine eigene Teilnehmerrufnummer. Bei Gruppenrufen werden diese Regeln ignoriert.

Bis zu 20 Teilnehmer pro Gruppenruf können eingerichtet werden.

Jedem Gruppenruf kann ein maximal 16 Zeichen langer Name zugewiesen werden.

Sprachbox für Gruppenruf

Bei der Einrichtung eines Gruppenrufs wird automatisch auch eine Sprachbox eingerichtet. Die Rufnummer dieser Gruppenruf-Sprachbox entspricht immer der Rufnummer des Gruppenrufs. Wird ein Gruppenruf von keinem Mitglied angenommen, erfolgt eine Rufweiterschaltung zur Gruppenruf-Sprachbox. Voraussetzung dafür ist, dass die Gruppenruf-Sprachbox als Rufweiterschaltungsziel dieses Gruppenrufs definiert wurde.

Nimmt ein Mitglied einen kommenden Anruf an seine eigene Teilnehmerrufnummer nicht an, wird dieser Anruf zu einem Rufweiterschaltungsziel entsprechend der Rufzielliste dieses Teilnehmers weitergeschaltet.

Beispiel für einen Gruppenruf des Typs Freifall mit der Gruppenrufnummer 404 und den Mitgliedern A (Teilnehmerrufnummer 200), B (201) und C (202). Für den Gruppenruf wurde eine Rufweiterschaltung nach Zeit zur Gruppenruf-Sprachbox eingerichtet. Jedes Mitglied hat eine Rufweiterschaltung nach Zeit zur eigenen Sprachbox definiert.		
Ankommender Anruf für Mitglied A (200)	Alle Mitglieder sind frei.	Mitglied A nimmt den Anruf nicht an. Es erfolgt eine Rufweiterschaltung nach Zeit zur Sprachbox des Mitglieds A.
	Mitglied A hat eine sofortige Rufweiterschaltung zur eigenen Sprachbox definiert. Mitglieder B und C sind frei.	Es erfolgt eine sofortige Rufweiterschaltung zur Sprachbox des Mitglieds A.
Ankommender Anruf für den Gruppenruf (404)	Alle Mitglieder sind frei.	Der Anruf wird bei allen Mitgliedern signalisiert. Kein Mitglied nimmt den Anruf an. Es erfolgt eine Rufweiterschaltung nach Zeit zur Gruppenruf-Sprachbox.
	Mitglied A hat eine sofortige Rufweiterschaltung zur eigenen Sprachbox definiert. Mitglieder B und C sind frei.	Der Anruf wird bei den Mitgliedern B und C signalisiert. Kein Mitglied nimmt den Anruf an. Es erfolgt eine Rufweiterschaltung nach Zeit zur Gruppenruf-Sprachbox.
	Mitglied A hat eine sofortige Rufweiterschaltung zu einem externen Ziel definiert. Mitglieder B und C sind frei.	Der Anruf wird bei den Mitgliedern B und C sowie beim externen Ziel signalisiert. Kein Mitglied nimmt den Anruf an. Es erfolgt eine Rufweiterschaltung nach Zeit zur Gruppenruf-Sprachbox.
	Mitglied A hat über den AutoAttendant Regeln zur Rufweiterschaltung definiert. Mitglieder B und C sind frei.	Der Anruf wird bei allen Mitgliedern signalisiert. Kein Mitglied nimmt den Anruf an. Es erfolgt eine Rufweiterschaltung nach Zeit zur Gruppenruf-Sprachbox.

Gruppenruf ein-/ausschalten

Ist ein Teilnehmer Mitglied eines Gruppenrufs, kann er sich mittels Kennzahlen aus dem Gruppenruf hinausschalten und wieder hineinschalten.

Ist ein Teilnehmer sowohl Mitglied mehrerer Gruppenrufe als auch Mitglied mehrerer Sammelanschlüsse, kann er sich über Kennzahlen aus allen Gruppenrufen und Sammelanschlüssen hinausschalten und wieder hineinschalten. Das Hinaus-/Hineinschalten aus einem bestimmten Gruppenruf oder Sammelanschluss ist über Kennzahlen und anschließender Auswahl aus den im Display angezeigten Gruppenrufen und Sammelanschlüssen möglich.

Möglich ist auch die Programmierung von Funktionstasten mit Umschaltfunktion für das Hinausschalten und Hineinschalten. Dabei kann eine Funktionstaste so programmiert werden, dass diese für einen bestimmten oder für alle Gruppenrufe und Sammelanschlüsse gilt. Auch eine variable Programmierung ist möglich. Nach Betätigung einer solchen Funktionstaste muss anschließend durch Auswahl aus den im Display angezeigten Gruppenrufen und Sammelan-

schlüssen definiert werden, für welchen Gruppenruf oder Sammelanschluss das Hinaus-/Hineinschalten gelten soll.

Rufart

Für jeden Gruppenruf kann ein Administrator mit dem Profil **Expert** die akustische Signalisierung kommender externer Anrufe über die Einstellung der Rufart definieren. Es bestehen folgende Möglichkeiten:

- Doppel-Rufton (Standardeinstellung)
- Dreifach-Rufton
- Kurz/Lang/Kurz-Rufton

Bei analogen Telefonen ist ausschließlich die Standardeinstellung möglich. Änderungen haben keine Auswirkung.

SIP-Telefone

Die Einbindung von SIP-Telefonen in einen Gruppenruf ist möglich.

> ***INFO:*** Bei SIP-Telefonen ist keine Programmierung von Funktionstasten möglich. Darüber hinaus können keine Leistungsmerkmale über Kennzahlen aktiviert oder deaktiviert werden. Spezifische Displaymeldungen eines Gruppenrufes werden nicht unterstützt.

Abhängigkeiten

Thema	Abhängigkeit
Anrufumleitung	Aktiviert ein Gruppenmitglied eine Anrufumleitung für alle Anrufe, werden alle Anrufe am Zieltelefon signalisiert.
Anrufschutz	Aktiviert ein Gruppenmitglied den Anrufschutz, werden ankommende Anrufe für sein Telefon nicht durchgestellt. Das betrifft Anrufe über die Gruppenrufnummer und die eigene Teilnehmerrufnummer.
Aufschalten	Sind alle Mitglieder eines Gruppenrufs besetzt, ist kein Aufschalten möglich.
ISDN-Telefone	Die Einbindung von ISDN-Telefonen in einen Gruppenruf ist nicht möglich.

Verwandte Themen

- Wie Sie einen Gruppenruf (Gruppe) hinzufügen
- Wie Sie einen Gruppenruf (Gruppe) ändern
- Wie Sie einen Gruppenruf (Gruppe) löschen
- Wie Sie ein Mitglied zum Gruppenruf (Gruppe) hinzufügen oder löschen
- Wie Sie einen Gruppenruf (Freifall oder Anklopfen) hinzufügen
- Wie Sie einen Gruppenruf (Freifall oder Anklopfen) anzeigen oder ändern

- Wie Sie einen Gruppenruf (Freifall oder Anklopfen) löschen
- Wie Sie ein Mitglied zum Gruppenruf (Freifall oder Anklopfen) hinzufügen oder löschen
- Wie Sie Anklopfschutz für Gruppenmitglied ein- oder ausschalten

14.1.3 Sammelanschluss

Sammelanschlüsse ermöglichen eine Verteilung der ankommenden Anrufe auf die zugehörigen Teilnehmer (Mitglieder). Ist ein Teilnehmer besetzt oder nimmt ein Teilnehmer einen kommenden Anruf nicht an, wird der Anruf automatisch zum nächsten freien Mitglied des Sammelanschlusses weitergeleitet. Alle Mitglieder des Sammelanschlusses sind unter einer Rufnummer erreichbar.

Jedes Mitglied eines Sammelanschlusses ist auch unter seiner eigenen Teilnehmerrufnummer erreichbar.

Dem Sammelanschluss muss eine der folgenden Eigenschaften zugewiesen werden.

- Linear
  Ein ankommender Anruf wird immer zuerst beim ersten Mitglied des Sammelanschlusses signalisiert. Die weitere Signalisierung erfolgt anhand der in der Gruppentabelle eingetragenen Reihenfolge der Mitglieder.
- Zyklisch
  Ein ankommender Anruf wird zuerst bei dem Mitglied signalisiert, der dem Teilnehmer nachfolgt, der den letzten Anruf angenommen hat. Die weitere Signalisierung erfolgt anhand der in der Gruppentabelle eingetragenen Reihenfolge der Mitglieder.

Die Weiterschaltung zum nächsten freien Mitglied des Sammelanschlusses erfolgt automatisch nach Ablauf der eingestellten Rufweiterschaltungszeit, sofern ein Anruf nicht angenommen wird oder ein Mitglied besetzt ist oder den Anklopfschutz aktiviert hat.

Für den Fall, dass ein Anruf von keinem Mitglied des Sammelanschlusses angenommen werden kann, kann ein Rufweiterschaltungsziel (Rufzielliste) definiert werden.

Ein einzelner Teilnehmer kann gleichzeitig mehreren Gruppen angehören. Für die Gruppen des Typs Gruppenruf, Sammelanschluss, Teamschaltung/Team-Gruppe und Chef/Sekretär/Top-Gruppe gilt: Die Summe aller Mitgliedschaften des Teilnehmers in diesen Gruppen darf 32 nicht übersteigen.

Im Display eines rufenden internen Teilnehmers wird der zugewiesene Name des Sammelanschlusses angezeigt. Nach Annahme eines Anrufs, wird der Name des Teilnehmers angezeigt, der den Anruf angenommen hat.

Hat ein Mitglied über den AutoAttendant Regeln definiert, zum Beispiel für die Weiterschaltung von Anrufen, gelten diese nur für Anrufe an seine eigene Teilnehmerrufnummer. Bei Anrufen für den Sammelanschluss werden diese Regeln ignoriert.

Bis zu 20 Teilnehmer pro Sammelanschluss können eingerichtet werden.

Jedem Sammelanschluss kann ein maximal 16 Zeichen langer Name zugewiesen werden.

Sprachbox für Sammelanschluss

Bei der Einrichtung eines Sammelanschlusses wird automatisch auch eine Sprachbox eingerichtet. Die Rufnummer dieser Sammelanschluss-Sprachbox entspricht immer der Rufnummer des Sammelanschlusses. Wird ein Anruf für einen Sammelanschluss von keinem Mitglied angenommen, erfolgt eine Rufweiterschaltung zur Sammelanschluss-Sprachbox. Voraussetzung dafür ist, dass die Sammelanschluss-Sprachbox als Rufweiterschaltungsziel dieses Sammelanschlusses definiert wurde.

Nimmt ein Mitglied einen kommenden Anruf an seine eigene Teilnehmerrufnummer nicht an, wird dieser Anruf zu einem Rufweiterschaltungsziel entsprechend der Rufzielliste dieses Teilnehmers weitergeschaltet.

Beispiel für einen linearen Sammelanschluss mit der Rufnummer 404 und den Mitgliedern A (Teilnehmerrufnummer 200), B (201) und C (202). Für den Sammelanschluss wurde eine Rufweiterschaltung nach Zeit zur Sammelanschluss-Sprachbox eingerichtet. Jedes Mitglied hat eine Rufweiterschaltung nach Zeit zur eigenen Sprachbox definiert.		
Ankommender Anruf für Mitglied A (200)	Alle Mitglieder sind frei.	Mitglied A nimmt den Anruf nicht an. Es erfolgt eine Rufweiterschaltung nach Zeit zur Sprachbox des Mitglieds A.
	Mitglied A hat eine sofortige Rufweiterschaltung zur eigenen Sprachbox definiert. Mitglieder B und C sind frei.	Es erfolgt eine sofortige Rufweiterschaltung zur Sprachbox des Mitglieds A.
Ankommender Anruf für den Sammelanschluss (404)	Alle Mitglieder sind frei.	Der Anruf wird zuerst bei Mitglied A, dann bei Mitglied B und dann bei Mitglied C signalisiert. Kein Mitglied nimmt den Anruf an. Es erfolgt eine Rufweiterschaltung nach Zeit zur Sammelanschluss-Sprachbox.
	Mitglied A hat eine sofortige Rufweiterschaltung zur eigenen Sprachbox definiert. Mitglieder B und C sind frei.	Der Anruf wird zuerst bei Mitglied B und dann bei Mitglied C signalisiert. Kein Mitglied nimmt den Anruf an. Es erfolgt eine Rufweiterschaltung nach Zeit zur Sammelanschluss-Sprachbox.
	Mitglied A hat eine sofortige Rufweiterschaltung zu einem externen Ziel definiert. Mitglieder B und C sind frei.	Der Anruf wird zuerst bei Mitglied B und dann bei Mitglied C signalisiert. Kein Mitglied nimmt den Anruf an. Es erfolgt eine Rufweiterschaltung nach Zeit zur Sammelanschluss-Sprachbox.
	Mitglied A hat über den AutoAttendant Regeln zur Rufweiterschaltung definiert. Mitglieder B und C sind frei.	Der Anruf wird zuerst bei Mitglied A, dann bei Mitglied B und dann bei Mitglied C signalisiert. Kein Mitglied nimmt den Anruf an. Es erfolgt eine Rufweiterschaltung nach Zeit zur Sammelanschluss-Sprachbox.

Sammelanschluss ein-/ausschalten

Ist ein Teilnehmer Mitglied eines Sammelanschlusses, kann er sich mittels Kennzahlen aus diesem Sammelanschluss hinausschalten und wieder hineinschalten.

Ist ein Teilnehmer sowohl Mitglied mehrerer Sammelanschlüsse als auch Mitglied mehrerer Gruppenrufe, kann er sich über Kennzahlen aus allen Sammelanschlüssen und Gruppenrufen hinausschalten und wieder hineinschalten. Das Hinaus-/Hineinschalten aus einem bestimmten Sammelanschluss oder Gruppenruf ist über Kennzahlen und anschließender Auswahl aus den im Display angezeigten Sammelanschlüssen und Gruppenrufen möglich.

Möglich ist auch die Programmierung von Funktionstasten mit Umschaltfunktion für das Hinausschalten und Hineinschalten. Dabei kann eine Funktionstaste so programmiert werden, dass diese für einen bestimmten oder für alle Sammelanschlüsse und Gruppenrufe gilt. Auch eine variable Programmierung ist möglich. Nach Betätigung einer solchen Funktionstaste muss anschließend durch Auswahl aus den im Display angezeigten Sammelanschlüssen und Gruppenrufen definiert werden, für welchen Sammelanschluss oder Gruppenruf das Hinaus-/Hineinschalten gelten soll.

Rufart

Für jeden Sammelanschluss kann ein Administrator mit dem Profil **Expert** die akustische Signalisierung kommender externer Anrufe über die Einstellung der Rufart definieren. Es bestehen folgende Möglichkeiten:

- Doppel-Rufton (Standardeinstellung)
- Dreifach-Rufton
- Kurz/Lang/Kurz-Rufton

Bei analogen Telefonen ist ausschließlich die Standardeinstellung möglich. Änderungen haben keine Auswirkung.

SIP-Telefone

Die Einbindung von SIP-Telefonen in einen Sammelanschluss ist möglich.

> ***INFO:*** Bei SIP-Telefonen ist keine Programmierung von Funktionstasten möglich. Darüber hinaus können keine Leistungsmerkmale über Kennzahlen aktiviert oder deaktiviert werden. Spezifische Displaymeldungen eines Sammelanschlusses werden nicht unterstützt.

Abhängigkeiten

Thema	Abhängigkeit
Anrufumleitung	Aktiviert ein Sammelanschlussmitglied eine Anrufumleitung für alle Anrufe, werden alle Anrufe am Zieltelefon signalisiert.
Anrufschutz	Aktiviert ein Sammelanschlussmitglied den Anrufschutz, werden ankommende Anrufe für sein Telefon nicht durchgestellt. Das betrifft Anrufe für den Sammelanschluss und die eigene Teilnehmerrufnummer.
Warteschlange	Für zyklische und lineare Sammelanschlüsse ist das Einrichten einer Warteschlange nicht möglich.
ISDN-Telefone	Die Einbindung von ISDN-Telefonen in Sammelanschlüsse ist nicht möglich.

Verwandte Themen

- Wie Sie einen Sammelanschluss hinzufügen
- Wie Sie einen Sammelanschluss ändern
- Wie Sie einen Sammelanschluss löschen
- Wie Sie ein Mitglied zum Sammelanschluss hinzufügen oder löschen

14.1.4 Konfiguration von Anrufübernahmegruppen, Gruppenrufen und Sammelanschlüssen über Wizards

Verschiedene Wizards ermöglichen die komfortable Konfiguration von Anrufübernahmegruppen, Gruppenrufen und Sammelanschlüssen.

Mit dem Wizard **Anrufübernahme** können Sie Teilnehmer zu einer Gruppe zusammenfassen, um eine gegenseitige Rufannahme zu ermöglichen. Beschrieben ist die Vorgehensweise für folgende Anwendungsfälle, die über den Wizard eingerichtet werden können:

- *Wie Sie Anrufübernahmegruppen konfigurieren*
- *Wie Sie ein Mitglied zur Anrufübernahmegruppe hinzufügen oder löschen*

Mit dem Wizard **Gruppenruf / Sammelanschluss** können Sie Gruppenrufe des Typs Gruppe und Sammelanschlüsse konfigurieren. Beschrieben ist die Vorgehensweise für folgende Anwendungsfälle, die über den Wizard eingerichtet werden können:

- *Wie Sie einen Gruppenruf (Gruppe) hinzufügen*
- *Wie Sie einen Gruppenruf (Gruppe) ändern*
- *Wie Sie einen Gruppenruf (Gruppe) löschen*
- *Wie Sie ein Mitglied zum Gruppenruf (Gruppe) hinzufügen oder löschen*
- *Wie Sie einen Sammelanschluss hinzufügen*
- *Wie Sie einen Sammelanschluss ändern*

- *Wie Sie einen Sammelanschluss löschen*
- *Wie Sie ein Mitglied zum Sammelanschluss hinzufügen oder löschen*

14.1.4.1 Wie Sie Anrufübernahmegruppen konfigurieren

Der Wizard **Anrufübernahme** ermöglicht Ihnen das Zusammenfassen von Teilnehmern zu einer Gruppe, mit der Möglichkeit der gegenseitigen Rufannahme.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > User-Telefonie**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Anrufübernahme** zu starten. Es wird Ihnen die Liste aller möglichen Anrufübernahmegruppen angezeigt.

4) Um eine Anrufübernahmegruppe zu konfigurieren, klicken Sie in der Zeile der gewünschten Anrufübernahmegruppe auf **Bearbeiten**.

5) Wenn Sie Mitglieder zu der Anrufübernahmegruppe hinzufügen möchten, aktivieren Sie die Kontrollkästchen **Zuordnung Gruppe <Nummer>** der gewünschten Rufnummern/Namen.

6) Wenn Sie Mitglieder aus der Anrufübernahmegruppe entfernen möchten, deaktivieren Sie die Kontrollkästchen **Zuordnung Gruppe <Nummer>** der gewünschten Rufnummern/Namen.

7) Klicken Sie auf **OK**, um die Eingaben zu übernehmen.

8) Geben Sie im Feld **Name** den Namen der soeben konfigurierten Anrufübernahmegruppe ein.

9) Wenn Sie weitere Anrufübernahmegruppen konfigurieren möchten, wiederholen Sie die Schritte 4 bis 8.

10) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

Verwandte Themen

- Anrufübernahmegruppe

14.1.4.2 Wie Sie ein Mitglied zur Anrufübernahmegruppe hinzufügen oder löschen

Mit dem Wizard **Anrufübernahme** können Sie Mitglieder zu Anrufübernahmegruppen hinzufügen oder löschen.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > User-Telefonie**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Anrufübernahme** zu starten.

4) Klicken Sie in der Zeile der gewünschten Anrufübernahmegruppe auf **Bearbeiten**.

5) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie Mitglieder zu der Anrufübernahmegruppe hinzufügen möchten, aktivieren Sie die Kontrollkästchen **Zuordnung Gruppe <Nummer>** der gewünschten Rufnummern/Namen.
- Wenn Sie Mitglieder aus der Anrufübernahmegruppe entfernen möchten, deaktivieren Sie die Kontrollkästchen **Zuordnung Gruppe <Nummer>** der gewünschten Rufnummern/Namen.

6) Klicken Sie auf **OK**, um die Eingaben zu bestätigen.

7) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

Verwandte Themen

- Anrufübernahmegruppe

14.1.4.3 Wie Sie einen Gruppenruf (Gruppe) hinzufügen

Mit dem Wizard **Gruppenruf / Sammelanschluss** können Sie Gruppenrufe des Typs Gruppe einrichten.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > User-Telefonie**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Gruppenruf / Sammelanschluss** zu starten.

4) Klicken Sie auf **Hinzufügen**, um einen neuen Gruppenruf einzurichten.

5) Geben Sie im Feld **Rufnummer der Gruppe** die Rufnummer des neuen Gruppenrufs ein.

6) Geben Sie im Feld **Durchwahlnummer** die Durchwahlnummer des neuen Gruppenrufs ein.

7) Geben Sie im Feld **Name der Gruppe** den Namen des neuen Gruppenrufs ein.

8) Wählen Sie in der Aufklappliste **Typ** den Eintrag **Gruppe** aus.

9) Wählen Sie eine der folgenden Möglichkeiten für die Übernahme der Rufnummer des Gruppenrufs in das interne Verzeichnis:

- Wenn die Rufnummer des Gruppenrufs im internen Verzeichnis erscheinen soll, aktivieren Sie das Kontrollkästchen **Tel.-Buch**.
- Wenn die Rufnummer des Gruppenrufs nicht im internen Verzeichnis erscheinen soll, deaktivieren Sie das Kontrollkästchen **Tel.-Buch**.

10) Wählen Sie in der Aufklappliste **Rufnummer des Teilnehmers, der der Gruppe zugeordnet werden soll** die Rufnummer des gewünschten Teilnehmers aus.

11) Klicken Sie auf **OK & Weiter**.

INFO: Ist die von Ihnen gewählte Rufnummer und/oder Durchwahlnummer bereits vorhanden, können Sie den aktuellen Rufnummernplan aufrufen, um eine freie Rufnummer und/oder Durchwahlnummer zu ermitteln.

---

12) Klicken Sie in der Zeile des neuen Gruppenrufs auf **Bearbeiten**, um dem Gruppenruf weitere Teilnehmer zuzuordnen.

13) Wählen Sie in der Aufklappliste **Ruf-Nr.** die Rufnummer des Teilnehmers aus, der dem Gruppenruf zugeordnet werden soll.

14) Klicken Sie auf **Hinzufügen**.

15) Wenn Sie dem Gruppenruf weitere Teilnehmer zuordnen möchten, wiederholen Sie die Schritte 13 und 14.

16) Klicken Sie auf **OK**, um die Eingaben zu übernehmen.

17) Wenn Sie einen weiteren Gruppenruf einrichten möchten, wiederholen Sie die Schritte 4 bis 16.

18) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

Verwandte Themen

- Gruppenruf

14.1.4.4 Wie Sie einen Gruppenruf (Gruppe) ändern

Mit dem Wizard **Gruppenruf / Sammelanschluss** können Sie Gruppenrufe des Typs Gruppe bearbeiten.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > User-Telefonie**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Gruppenruf / Sammelanschluss** zu starten.

4) Klicken Sie in der Zeile des zu ändernden Gruppenrufs auf **Bearbeiten**.

5) Ändern Sie die gewünschten Gruppenparameter.

6) Nur bei UC Smart: Ordnen Sie bei Bedarf dem Gruppenruf eine Mailbox zu:

a) Wählen Sie in der Aufklappliste **Mailboxtyp UC Smart** aus, ob der Gruppenruf eine Standardmailbox oder eine Vermittlungsmailbox (AutoAttendant) erhalten soll.

b) Nur bei Standardmailbox: Wenn ein Anrufer eine Nachricht auf der Sprachbox hinterlassen darf, aktivieren Sie das Kontrollkästchen **Aufnahme**.

c) Wählen Sie aus der Aufklappliste **Begrüßung** eine Begrüßung aus.

d) Wenn das Kennwort der Sprachbox zurückgesetzt werden soll, aktivieren Sie das Kontrollkästchen **Passwort Reset**.

INFO: Das Kontrollkästchen **Passwort Reset** muss bei einer Neueinrichtung einer Sprachbox nicht gesetzt sein. Es bewirkt das Rücksetzen des Kennworts der Sprachbox. Bei einer Neueinrichtung muss der Teilnehmer sowieso beim ersten Zugriff auf seine Sprachbox das Initial-Kennwort ändern.

---

7) Wenn Sie ein Mitglied zum Gruppenruf hinzufügen möchten, wählen Sie in der Aufklappliste **Ruf-Nr.** die Rufnummer des gewünschten Teilnehmers aus. Klicken Sie auf **Hinzufügen**.

8) Wenn Sie ein Mitglied aus dem Gruppenruf entfernen möchten, klicken Sie in der Zeile des gewünschten Gruppenmitglieds auf **Löschen** und anschließend auf **OK**.

9) Klicken Sie auf **OK**, um die Eingaben zu bestätigen.

10) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

Verwandte Themen

- Gruppenruf

14.1.4.5 Wie Sie einen Gruppenruf (Gruppe) löschen

Mit dem Wizard **Gruppenruf / Sammelanschluss** können Sie Gruppenrufe des Typs Gruppe löschen.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > User-Telefonie**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Gruppenruf / Sammelanschluss** zu starten.

4) Klicken Sie in der Zeile des zu löschenden Gruppenrufs auf **Bearbeiten**.

5) Klicken Sie auf **Daten löschen**.

6) Klicken Sie auf **OK**, um das Löschen zu bestätigen.

7) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

Verwandte Themen

- Gruppenruf

14.1.4.6 Wie Sie ein Mitglied zum Gruppenruf (Gruppe) hinzufügen oder löschen

Mit dem Wizard **Gruppenruf / Sammelanschluss** können Sie Mitglieder zu Gruppenrufen des Typs Gruppe hinzufügen oder löschen.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > User-Telefonie**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Gruppenruf / Sammelanschluss** zu starten.

4) Klicken Sie in der Zeile des gewünschten Gruppenrufs auf **Bearbeiten**.

5) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie ein Mitglied zum Gruppenruf hinzufügen möchten, wählen Sie in der Aufklappliste **Ruf-Nr.** die Rufnummer des gewünschten Teilnehmers aus. Klicken Sie auf **Hinzufügen**.

- Wenn Sie ein Mitglied aus dem Gruppenruf entfernen möchten, klicken Sie in der Zeile des gewünschten Gruppenmitglieds auf **Löschen** und anschließend auf **OK**.

6) Klicken Sie auf **OK**, um die Eingaben zu bestätigen.

7) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

Verwandte Themen

- Gruppenruf

14.1.4.7 Wie Sie einen Sammelanschluss hinzufügen

Mit dem Wizard **Gruppenruf / Sammelanschluss** können Sie Sammelanschlüsse einrichten.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > User-Telefonie**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Gruppenruf / Sammelanschluss** zu starten.

4) Klicken Sie auf **Hinzufügen**, um einen neuen Sammelanschluss einzurichten.

5) Geben Sie im Feld **Rufnummer der Gruppe** die Rufnummer des neuen Sammelanschlusses ein.

6) Geben Sie im Feld **Durchwahlnummer** die Durchwahlnummer des neuen Sammelanschlusses ein.

7) Geben Sie im Feld **Name der Gruppe** den Namen des neuen Sammelanschlusses ein.

8) Wählen Sie in der Aufklappliste **Typ** den Typ des neuen Sammelanschlusses aus. Sie haben folgende Möglichkeiten:

- Wenn ein Anruf immer zuerst beim ersten Mitglied des Sammelanschlusses signalisiert werden soll, wählen Sie den Eintrag **Linearer Sammelanschluss** aus.
- Wenn ein Anruf zuerst bei dem Mitglied signalisiert werden soll, der dem Teilnehmer nachfolgt, der den letzten Anruf angenommen hat, wählen Sie den Eintrag **Zyklischer Sammelanschluss** aus.

9) Wählen Sie eine der folgenden Möglichkeiten für die Übernahme der Rufnummer des Sammelanschlusses in das interne Verzeichnis:

- Wenn die Rufnummer des Sammelanschlusses im internen Verzeichnis erscheinen soll, aktivieren Sie das Kontrollkästchen **Tel.-Buch**.
- Wenn die Rufnummer des Sammelanschlusses nicht im internen Verzeichnis erscheinen soll, deaktivieren Sie das Kontrollkästchen **Tel.-Buch**.

10) Wählen Sie in der Aufklappliste **Rufnummer des Teilnehmers, der der Gruppe zugeordnet werden soll** die Rufnummer des gewünschten Teilnehmers aus.

11) Klicken Sie auf **OK & Weiter**.

INFO: Ist die von Ihnen gewählte Rufnummer und/oder Durchwahlnummer bereits vorhanden, können Sie den aktuellen Rufnummernplan aufrufen, um eine freie Rufnummer und/oder Durchwahlnummer zu ermitteln.

---

12) Klicken Sie in der Zeile des neuen Sammelanschlusses auf **Bearbeiten**, um dem Sammelanschluss weitere Teilnehmer zuzuordnen.

13) Wählen Sie in der Aufklappliste **Ruf-Nr.** die Rufnummer des Teilnehmers aus, der dem Sammelanschluss zugeordnet werden soll.

14) Klicken Sie auf **Hinzufügen**.

15) Wenn Sie dem Sammelanschluss weitere Teilnehmer zuordnen möchten, wiederholen Sie die Schritte 13 und 14.

16) Klicken Sie auf **OK**, um die Eingaben zu übernehmen.

17) Wenn Sie einen weiteren Sammelanschluss einrichten möchten, wiederholen Sie die Schritte 4 bis 16.

18) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

Verwandte Themen

- Sammelanschluss

14.1.4.8 Wie Sie einen Sammelanschluss ändern

Mit dem Wizard **Gruppenruf / Sammelanschluss** können Sie Sammelanschlüsse bearbeiten.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > User-Telefonie**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Gruppenruf / Sammelanschluss** zu starten.

4) Klicken Sie in der Zeile des zu ändernden Sammelanschlusses auf **Bearbeiten**.

5) Ändern Sie die gewünschten Parameter des Sammelanschlusses.

6) Nur bei UC Smart: Ordnen Sie bei Bedarf dem Sammelanschluss eine Mailbox zu:

a) Wählen Sie in der Aufklappliste **Mailboxtyp UC Smart** aus, ob der Sammelanschluss eine Standardmailbox oder eine Vermittlungsmailbox (AutoAttendant) erhalten soll.

b) Nur bei Standardmailbox: Wenn ein Anrufer eine Nachricht auf der Sprachbox hinterlassen darf, aktivieren Sie das Kontrollkästchen **Aufnahme**.

c) Wählen Sie aus der Aufklappliste **Begrüßung** eine Begrüßung aus.

d) Wenn das Kennwort der Sprachbox zurückgesetzt werden soll, aktivieren Sie das Kontrollkästchen **Passwort Reset**.

INFO: Das Kontrollkästchen **Passwort Reset** muss bei einer Neueinrichtung einer Sprachbox nicht gesetzt sein. Es bewirkt das Rücksetzen des Kennworts der Sprachbox. Bei einer Neueinrichtung muss der Teilnehmer sowieso beim ersten Zugriff auf seine Sprachbox das Initial-Kennwort ändern.

---

7) Wenn Sie ein Mitglied zum Sammelanschluss hinzufügen möchten, wählen Sie in der Aufklappliste **Ruf-Nr.** die Rufnummer des gewünschten Teilnehmers aus. Klicken Sie auf **Hinzufügen**.

8) Wenn Sie ein Mitglied aus dem Sammelanschluss entfernen möchten, klicken Sie in der Zeile des gewünschten Gruppenmitglieds auf **Löschen** und anschließend auf **OK**.

9) Wenn Sie die Position der Mitglieder innerhalb des Sammelanschlusses ändern möchten, klicken Sie auf **Reihenfolge ändern**. Geben Sie im Feld **Position** für jedes Mitglied die gewünschte Positionsnummer ein. Klicken Sie auf **OK & Weiter**.

10) Klicken Sie auf **OK**, um die Eingaben zu bestätigen.

11) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

Verwandte Themen

- Sammelanschluss

14.1.4.9 Wie Sie einen Sammelanschluss löschen

Mit dem Wizard **Gruppenruf / Sammelanschluss** können Sie Sammelanschlüsse löschen.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards > User-Telefonie**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Gruppenruf / Sammelanschluss** zu starten.
4) Klicken Sie in der Zeile des zu löschenden Sammelanschlusses auf **Bearbeiten**.
5) Klicken Sie auf **Daten löschen**.
6) Klicken Sie auf **OK**, um das Löschen zu bestätigen.
7) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

Verwandte Themen

- Sammelanschluss

14.1.4.10 Wie Sie ein Mitglied zum Sammelanschluss hinzufügen oder löschen

Mit dem Wizard **Gruppenruf / Sammelanschluss** können Sie Mitglieder zu Sammelanschlüssen hinzufügen oder löschen.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards > User-Telefonie**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Gruppenruf / Sammelanschluss** zu starten.
4) Klicken Sie in der Zeile des gewünschten Sammelanschlusses auf **Bearbeiten**.
5) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie ein Mitglied zum Sammelanschluss hinzufügen möchten, wählen Sie in der Aufklappliste **Ruf-Nr.** die Rufnummer des gewünschten Teilnehmers aus. Klicken Sie auf **Hinzufügen**.
   - Wenn Sie ein Mitglied aus dem Sammelanschluss entfernen möchten, klicken Sie in der Zeile des gewünschten Gruppenmitglieds auf **Löschen** und anschließend auf **OK**.

6) Klicken Sie auf **OK**, um die Eingaben zu bestätigen.

7) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

Verwandte Themen

- Sammelanschluss

14.1.5 Konfiguration von Anrufübernahmegruppen, Gruppenrufen und Sammelanschlüssen über Experten-Modus

Neben den Konfigurationsmöglichkeiten über Wizards stehen einem Administrator mit dem Profil **Expert** zusätzliche Möglichkeiten zur Konfiguration von Anrufübernahmegruppen, Gruppenrufen und Sammelanschlüssen über den **Experten-Modus** zur Verfügung.

Beschrieben ist die Vorgehensweise für folgende Anwendungsfälle, die über den **Experten-Modus** eingerichtet werden können:

- *Wie Sie die Anzeige der Rufnummer und des Namens des Anrufers aktivieren oder deaktivieren*
- *Wie Sie den Aufmerksamkeitston aktivieren oder deaktivieren*
- *Wie Sie die Anrufübernahme von Wiederanrufen aktivieren oder deaktivieren*
- *Wie Sie einen Gruppenruf (Freifall oder Anklopfen) hinzufügen*
- *Wie Sie einen Gruppenruf (Freifall oder Anklopfen) anzeigen oder ändern*
- *Wie Sie einen Gruppenruf (Freifall oder Anklopfen) löschen*
- *Wie Sie ein Mitglied zum Gruppenruf (Freifall oder Anklopfen) hinzufügen oder löschen*
- *Wie Sie Anklopfschutz für Gruppenmitglied ein- oder ausschalten*

14.1.5.1 Wie Sie die Anzeige der Rufnummer und des Namens des Anrufers aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **System > System Flags**.

4) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Rufnummer und Name des Anrufers angezeigt werden sollen, aktivieren Sie das Kontrollkästchen **A-Rufnummer in AUN-Gruppen / Rufzuschaltung / Umleitungsziel / RWS-Ziel**.
- Wenn Rufnummer und Name des Anrufers nicht angezeigt werden sollen, deaktivieren Sie das Kontrollkästchen **A-Rufnummer in AUN-Gruppen / Rufzuschaltung / Umleitungsziel / RWS-Ziel**.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Verwandte Themen

- Anrufübernahmegruppe

14.1.5.2 Wie Sie den Aufmerksamkeitston aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **System > System Flags**.

4) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie den Aufmerksamkeitston einschalten möchten, aktivieren Sie das Kontrollkästchen **Aufmerksamkeitssignalisierung bei AUN-Gruppen**.
- Wenn Sie den Aufmerksamkeitston ausschalten möchten, deaktivieren Sie das Kontrollkästchen **Aufmerksamkeitssignalisierung bei AUN-Gruppen**.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Verwandte Themen

- Anrufübernahmegruppe

14.1.5.3 Wie Sie die Anrufübernahme von Wiederanrufen aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **System > System Flags**.
4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn die Anrufübernahme von Wiederanrufen möglich sein soll, aktivieren Sie das Kontrollkästchen **Anrufübernahme nach Wiederanruf**.
   - Wenn die Anrufübernahme von Wiederanrufen nicht möglich sein soll, deaktivieren Sie das Kontrollkästchen **Anrufübernahme nach Wiederanruf**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Verwandte Themen

- Anrufübernahmegruppe

14.1.5.4 Wie Sie einen Gruppenruf (Freifall oder Anklopfen) hinzufügen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Kommende Rufe**.
3) Klicken Sie im Menübaum auf **Kommende Rufe > Gruppen-/Sammelanschluss**.
4) Klicken Sie auf die Registerkarte **Gruppe hinzufügen**.
5) Geben Sie im Feld **Rufnummer** die Rufnummer des neuen Gruppenrufs ein.
6) Geben Sie im Feld **Durchwahlnummer** die Durchwahlnummer des neuen Gruppenrufs ein.
7) Geben Sie im Feld **Name** den Namen des neuen Gruppenrufs ein.
8) Wählen Sie in der Aufklappliste **Typ** eine der folgenden Möglichkeiten aus:
   - Wenn Sie einen Gruppenruf des Typs Freifall einrichten möchten, wählen Sie den Eintrag **Freifall** aus.
   - Wenn Sie einen Gruppenruf des Typs Anklopfen einrichten möchten, wählen Sie den Eintrag **Anklopfen** aus.
9) Wählen Sie in der Aufklappliste **Rufnummer** die Rufnummer des Teilnehmers aus, der dem Gruppenruf zugeordnet werden soll.

10) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Verwandte Themen

- Gruppenruf

14.1.5.5 Wie Sie einen Gruppenruf (Freifall oder Anklopfen) anzeigen oder ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Kommende Rufe**.

3) Navigieren Sie im Menübaum unter **Kommende Rufe > Gruppen-/Sammelanschluss > …** zum gewünschten Gruppenruf.

4) Klicken Sie auf die Registerkarte **Gruppen-Parameter ändern**. Ihnen werden die aktuellen Einstellungen der Gruppen-Parameter angezeigt.

5) Ändern Sie bei Bedarf die gewünschten Parameter des Gruppenrufs.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Verwandte Themen

- Gruppenruf

14.1.5.6 Wie Sie einen Gruppenruf (Freifall oder Anklopfen) löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Kommende Rufe**.

3) Navigieren Sie im Menübaum unter **Kommende Rufe > Gruppen-/Sammelanschluss > …** zum gewünschten Gruppenruf.

4) Klicken Sie auf die Registerkarte **Gruppe löschen**.

5) Klicken Sie auf **Löschen** und anschließend auf **OK**.

Verwandte Themen

- Gruppenruf

14.1.5.7 Wie Sie ein Mitglied zum Gruppenruf (Freifall oder Anklopfen) hinzufügen oder löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Kommende Rufe**.

3) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie ein Mitglied zum Gruppenruf hinzufügen möchten, navigieren Sie im Menübaum unter **Kommende Rufe > Gruppen-/Sammelanschluss > …** zum gewünschten Gruppenruf. Klicken Sie auf die Registerkarte **Mitglied hinzufügen**. Wählen Sie in der Aufklappliste **Rufnummer** die Rufnummer des gewünschten Teilnehmers aus. Klicken Sie auf **Übernehmen** und anschließend auf **OK**.
- Wenn Sie ein Mitglied aus dem Gruppenruf entfernen möchten, navigieren Sie im Menübaum unter **Kommende Rufe > Gruppen-/Sammelanschluss > …** zum gewünschten Mitglied des Gruppenrufs ((Gruppenmitglied) Rufnummer Name). Klicken Sie auf die Registerkarte **Mitglied löschen**. Klicken Sie auf **Löschen** und anschließend auf **OK**.

Verwandte Themen

- Gruppenruf

14.1.5.8 Wie Sie Anklopfschutz für Gruppenmitglied ein- oder ausschalten

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Teilnehmer**.

3) Navigieren Sie im Menübaum unter **Teilnehmer > Teilnehmer > ...** zum gewünschten Teilnehmer (Index-Rufnummer-Name).

4) Klicken Sie auf die Registerkarte **Teilnehmer-Flags ändern**.

5) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie den Anklopfschutz einschalten möchten, aktivieren Sie das Kontrollkästchen **Anklopfschutz ein**.
- Wenn Sie den Anklopfschutz ausschalten möchten, deaktivieren Sie das Kontrollkästchen **Anklopfschutz ein**.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Verwandte Themen

- Gruppenruf

14.2 Teamschaltung / Team-Gruppe und Chef/Sekretär / Top-Gruppe

Eine Teamschaltung / Team-Gruppe bietet komfortable Funktionen für Teams. Die Rufnummern aller Teammitglieder werden auf MULAP-Tasten (Leitungstasten) programmiert. Damit hat jedes Teammitglied Zugriff auf alle Leitungen (zum Beispiel zur Anrufübernahme) und kann auch gleichzeitig über mehrere Leitungen telefonieren. Eine Chef/Sekretär / Top-Gruppe bietet komfortable Chef- und Sekretär-Funktionen (Topfunktion) für bis zu drei Chefs und bis zu drei Sekretäre.

14.2.1 Teamschaltung / Team-Gruppe

Bei einem Telefon mit Funktionen für Teams werden die eigene und die Rufnummern der weiteren Teammitglieder auf MULAP (Multiple Line Appearance)-Tasten (Leitungstasten) programmiert. Jedes Teammitglied hat Zugriff auf alle Leitungen (z. B. zur Anrufübernahme) und kann auch gleichzeitig über mehrere Leitungen telefonieren. Darüber hinaus werden automatisch Direktruftasten programmiert, über die die Teammitglieder sich direkt anrufen können.

Über die MULAP-Tasten haben die Teammitglieder Zugriff auf die Rufnummern aller Mitglieder. Ein kommender Anruf für ein Teammitglied kann dementsprechend auch von allen anderen Mitgliedern durch Drücken der blinkenden MULAP-Taste angenommen werden. Ebenso möglich ist das Makeln zwischen mehreren Leitungen. Durch Drücken einer MULAP-Taste kann ein Teammitglied einen gehenden Anruf über die zugehörige Leitung tätigen. Dem Angerufenen wird die zu dieser Leitung gehörende Rufnummer im Display angezeigt.

Ankommende Anrufe werden gleichzeitig bei allen Teammitgliedern optisch, über die LED der MULAP-Taste signalisiert. Für jedes Teammitglied kann zusätzlich angegeben werden, ob ankommende Anrufe auch akustisch signalisiert werden sollen.

Über eine Gruppenruftaste kann jedes Teammitglied die Signalisierung der ankommenden Anrufe für jede einzelne Leitung ein- oder ausschalten.

Bis zu drei Teilnehmer pro Teamschaltung/Team-Gruppe kann ein Administrator mit dem Profil **Advanced** über den Wizard **Teamschaltung** einrichten. Bis zu zehn Teilnehmer pro Teamschaltung/Team-Gruppe kann ein Administrator mit dem Profil **Expert** über den **Experten-Modus** einrichten.

Ein einzelner Teilnehmer kann gleichzeitig mehreren Gruppen angehören. Für die Gruppen des Typs Gruppenruf, Sammelanschluss, Teamschaltung/Team-Gruppe und Chef/Sekretär/Top-Gruppe gilt: Die Summe aller Mitgliedschaften des Teilnehmers in diesen Gruppen darf 32 nicht übersteigen.

Jeder Teamschaltung/Team-Gruppe kann ein maximal 16 Zeichen langer Name zugewiesen werden.

Bei der Einrichtung einer Teamschaltung/Team-Gruppe werden den Mitgliedern folgende Eigenschaften zugewiesen (Änderungen der Einstellungen können durch einen Administrator mit dem Profil **Expert** über den **Experten-Modus** durchgeführt werden.):

- **Master**
  Durch diesen Parameter wird ein Mitglied zu einem Master der Teamschaltung/Team-Gruppe. Aktiviert ein Master eine Anrufumleitung, gilt diese für alle Mitglieder (Telefone) der Teamschaltung/Team-Gruppe.
  Standardeinstellung: Master ist das erste Mitglied der Teamschaltung/Team-Gruppe.
- **Akustischer Ruf**
  Ist dieser Parameter aktiviert, werden ankommende Anrufe akustisch signalisiert.
  Standardeinstellung: Der Parameter ist aktiviert.
- **Automatische Belegung gehend**
  Ist dieser Parameter aktiviert, wird beim Abheben des Hörers automatisch über die MULAP-Leitung dieses Mitglieds gerufen. Bei nicht aktiviertem Parameter muss der Teilnehmer die MULAP-Taste betätigen, bevor er wählen kann.
  Standardeinstellung: Der Parameter ist aktiviert.
- **Keine automatische Rufannahme kommend**
  Ist dieser Parameter aktiviert, kann ein kommender Anruf nicht durch Abheben des Hörers angenommen werden. Ein kommender Anruf muss durch Betätigen der MULAP-Taste angenommen werden.
  Standardeinstellung: Der Parameter ist nicht aktiviert.
- **Automatische Konferenzfreigabe**
  Bei aktiviertem Parameter wird durch Drücken der MULAP-Taste die belegte MULAP-Leitung für eine Konferenz freigegeben. Bei allen weiteren Mitgliedern wird die Freigabe durch Blinken der MULAP-Taste angezeigt. Durch das Drücken der MULAP-Taste können sie sich in die Konferenz hineinschalten.
  Standardeinstellung: Der Parameter ist nicht aktiviert.
- **MULAP-Taste eingerichtet**
  Bei aktiviertem Parameter wird bei dem zugehörigen Telefon eine MULAP-Taste eingerichtet. Durch Drücken der Taste erfolgt eine gehende Belegung über die MULAP-Leitung des Masters. Dem Angerufenen wird die MULAP-Rufnummer des Masters im Display angezeigt.
  Standardeinstellung: Der Parameter ist nicht aktiviert.

MULAP-Tasten nutzen

Jedem Teammitglied ist eine eigene Leitung (MULAP-Leitung) zugeordnet. Die eigene und die Leitungen aller anderen Mitglieder sind bei jedem Teammitglied als MULAP-Tasten (Leitungstasten) eingerichtet. Somit kann jedes Teammitglied alle vorhandenen MULAP-Leitungen nutzen.

Die LED einer MULAP-Taste (Leitungstaste) hat folgende Bedeutung:

- Aus: Die zugehörige Leitung ist frei und kann verwendet werden.
- Leuchtet: Die zugehörige Leitung ist belegt.
- Blinkt schnell: Anruf auf der zugehörigen Leitung.
- Blinkt langsam: Ein gehaltenes Gespräch wartet auf der zugehörigen Leitung.

Direktruftasten nutzen

Jedes Teammitglied hat für jedes andere Teammitglied eine Direktruftaste. Somit sind die Teammitglieder untereinander direkt per Tastendruck erreichbar.

Eine Direktruftaste kann auch verwendet werden, um ein bestehendes Gespräch schnell an das darunter programmierte Teammitglied zu übergeben.

Die LED einer Direktruftaste hat folgende Bedeutung:

- Aus: Das zugehörige Teammitglied telefoniert nicht.
- Leuchtet: Das zugehörige Teammitglied telefoniert oder hat Anrufschutz eingeschaltet.
- Blinkt schnell: Das zugehörige Teammitglied ruft an. Der Anruf kann durch Drücken der Direktruftaste angenommen werden.
- Blinkt langsam: Das zugehörige Teammitglied wird gerufen und hat den Anruf noch nicht angenommen. Der Anruf kann durch Drücken der Direktruftaste übernommen werden.

Rufart

Für jede Teamschaltung/Team-Gruppe kann ein Administrator mit dem Profil **Expert** die akustische Signalisierung kommender externer Anrufe über die Einstellung der Rufart definieren. Es bestehen folgende Möglichkeiten:

- Doppel-Rufton (Standardeinstellung)
- Dreifach-Rufton
- Kurz/Lang/Kurz-Rufton

Bei analogen Telefonen ist ausschließlich die Standardeinstellung möglich. Änderungen haben keine Auswirkung.

Faxbox für Teamschaltung/Team-Gruppe

Für jede Teamschaltung/Team-Gruppe kann eine Faxbox eingerichtet werden, über die die Mitglieder Faxnachrichten direkt über myPortal for Desktop oder myPortal for Outlook empfangen können.

Wurde für den Master (das erste Mitglied) der Teamschaltung/Team-Gruppe bereits eine Faxbox konfiguriert, wird diese Faxbox bei der Einrichtung der Teamschaltung/Team-Gruppe übernommen. Bereits konfigurierte Faxboxen der anderen Mitglieder werden gelöscht.

Nach dem Auflösen einer Teamschaltung/Team-Gruppe kann nur noch der ehemalige Master (das erste Mitglied) die Faxbox nutzen.

SIP-Telefone

Die Einbindung von SIP-Telefonen in eine Teamschaltung/Team-Gruppe ist möglich. Voraussetzung dafür ist, dass als erstes Mitglied der Teamschaltung/ Team-Gruppe ein Systemtelefon (zum Beispiel IP-Telefon, HFA) definiert wird.

Eingebunden werden können beispielsweise Dual-Mode-Mobiltelefone, die als Mobility Entry-Teilnehmer eingerichtet sind. Dual-Mode-Mobiltelefone unterstützen sowohl GSM/UMTS-Netze als auch WLAN-Netze. Über WLAN ist die Registrierung eines Dual-Mode-Mobiltelefons als IP-Teilnehmer (SIP Client) am Kommunikationssystem möglich.

INFO: Bei SIP-Telefonen ist keine Programmierung von MULAP-Tasten und Direktruftasten möglich. Darüber hinaus können keine Leistungsmerkmale über Kennzahlen aktiviert oder deaktiviert werden. Spezifische Displaymeldungen der Teamschaltung/ Team-Gruppe werden nicht unterstützt.

Abhängigkeiten

Thema	Abhängigkeit
Anrufumleitung	Ein Teammitglied hat eine Anrufumleitung für alle Anrufe aktiviert. In diesem Fall werden alle Anrufe für seine eigene Teilnehmerrufnummer umgeleitet.
Anrufschutz	Aktiviert ein Teammitglied den Anrufschutz, werden ankommende Anrufe nicht durchgestellt.
ISDN-Telefone	Die Einbindung von ISDN-Telefonen in Teamschaltungen/ Team-Gruppen ist nicht möglich.

14.2.2 Chef/Sekretär / Top-Gruppe

Top-Gruppen können eingerichtet werden, wenn komfortable Chef- und Sekretär-Funktionen (Topfunktion) benötigt werden.

Chef-Sekretär-Funktionen können für Gruppen mit bis zu drei Chefs und bis zu drei Sekretären eingerichtet werden.

INFO: Die Formulierungen “der Chef” und “der Sekretär” gelten auch für Gruppen mit mehr als einem Chef und mehr als einem Sekretär. In diesem Text steht "der Chef” stellvertretend sowohl für Chef als auch Chefin und “der Sekretär” stellvertretend sowohl für Sekretär als auch Sekretärin.

Jedem Topmitglied (jedem Chef und jedem Sekretär) ist eine eigene Leitung, die sogenannte MULAP (Multiple Line Appearance)-Leitung zugeordnet. Die eigene und die MULAP-Leitungen aller anderen Mitglieder sind bei jedem Topmitglied als MULAP-Tasten (Leitungstasten) eingerichtet. Bei gehenden Anrufen über die MULAP-Leitung wird den Angerufenen die MULAP-Rufnummer im Display angezeigt. Der Sekretär kann gehende Anrufe über seine eigene oder über die MULAP-Leitung aller Chefs und anderer Sekretäre tätigen. Soll beispielsweise eine Verbindung für einen Chef aufgebaut werden, könnte dafür die MULAP-Leitung dieses Chefs genutzt werden.

Darüber hinaus werden Direktruftasten programmiert, über die der Chef den Sekretär und umgekehrt direkt anrufen kann.

Ankommende Anrufe werden gleichzeitig bei allen Topmitgliedern optisch, über die LED der Leitungstaste signalisiert. Für jedes Topmitglied kann zusätzlich angegeben werden, ob ankommende Anrufe auch akustisch signalisiert werden sollen. Dabei erfolgt die akustische Signalisierung in Abhängigkeit von der Rufumschaltetaste.

Über eine Rufumschaltetaste kann die Signalisierung der ankommenden Anrufe umgeschaltet werden. Ankommende Anrufe werden entweder beim Chef oder beim Sekretär signalisiert. Betätigt der Chef die Rufumschaltetaste, werden ihm ankommende Anrufe weiterhin über Popup-Fenster angezeigt. Die Annahme eines Anrufes ist aber nur über eine entsprechende Taste am Telefon und nicht über das Popup-Fenster möglich.

Sekretär-Telefone können sich über eine Gruppenruftaste aus der Chef/Sekretär-Konfiguration/Top-Gruppe hinaus- und wieder hineinschalten. Dabei hat die Rufumschaltung Priorität.

INFO: Schaltet sich der Sekretär mit der Gruppenruftaste aus der Chef/Sekretär-Konfiguration/Top-Gruppe hinaus, ohne die Rufumschaltung für den Chef zu aktivieren, werden ankommende Anrufe weder beim Chef noch beim Sekretär signalisiert.

Bis zu zwei Chefs und bis zu zwei Sekretäre pro Chef/Sekretär-Konfiguration/Top-Gruppe kann ein Administrator mit dem Profil **Advanced** über den Wizard **Chef / Sekretär** einrichten. Bis zu drei Chefs und bis zu drei Sekretäre pro Chef/Sekretär-Konfiguration/Top-Gruppe kann ein Administrator mit dem Profil **Expert** über den **Experten-Modus** einrichten.

Für jeden Chef können maximal drei Telefone und für jeden Sekretär können maximal zwei Telefone eingerichtet werden.

Ein einzelner Teilnehmer kann gleichzeitig mehreren Gruppen angehören. Für die Gruppen des Typs Gruppenruf, Sammelanschluss, Teamschaltung/Team-Gruppe und Chef/Sekretär/Top-Gruppe gilt: Die Summe aller Mitgliedschaften des Teilnehmers in diesen Gruppen darf 32 nicht übersteigen.

Jeder Chef/Sekretär-Konfiguration/Top-Gruppe kann ein maximal 16 Zeichen langer Name zugewiesen werden.

Bei der Einrichtung einer Chef/Sekretär-Konfiguration/Top-Gruppe werden den Mitgliedern folgende Eigenschaften zugewiesen (Änderungen der Einstellungen

können durch einen Administrator mit dem Profil **Expert** über den **Experten-Modus** durchgeführt werden.):

- **Master**
  Durch diesen Parameter erhält ein Mitglied Chef-Funktionen. Beim Abheben des Hörers wird automatisch über die MULAP-Leitung dieses Mitglieds gerufen. Ankommende Anrufe über die zugehörige Chef-MULAP-Rufnummer werden standardmäßig ausschließlich optisch signalisiert.
  Standardeinstellung: Chef-Funktionen erhalten alle Chefs der Chef/Sekretär-Konfiguration/Top-Gruppe.
- **Akustischer Ruf**
  Ist dieser Parameter aktiviert, werden ankommende Anrufe akustisch signalisiert.
  Standardeinstellung: Der Parameter ist für alle Mitglieder mit Sekretär-Funktion aktiviert.
- **Automatische Belegung gehend**
  Ist dieser Parameter aktiviert, wird beim Abheben des Hörers automatisch über die MULAP-Leitung dieses Mitglieds gerufen. Bei nicht aktiviertem Parameter muss der Teilnehmer die MULAP-Taste betätigen, bevor er wählen kann.
  Standardeinstellung: Der Parameter ist für alle Mitglieder aktiviert.
- **Keine automatische Rufannahme kommend**
  Ist dieser Parameter aktiviert, kann ein kommender Anruf nicht durch Abheben des Hörers angenommen werden. Ein kommender Anruf muss durch Betätigen der MULAP-Taste angenommen werden.
  Standardeinstellung: Der Parameter ist nicht aktiviert.
- **Automatische Konferenzfreigabe**
  Bei aktiviertem Parameter wird durch Drücken der MULAP-Taste die belegte MULAP-Leitung für eine Konferenz freigegeben. Bei allen weiteren Mitgliedern wird die Freigabe durch Blinken der MULAP-Taste angezeigt. Durch das Drücken der MULAP-Taste können sie sich in die Konferenz hineinschalten.
  Standardeinstellung: Der Parameter ist nicht aktiviert.
- **MULAP-Taste eingerichtet**
  Bei aktiviertem Parameter wird bei dem zugehörigen Telefon eine MULAP-Taste eingerichtet. Durch Drücken der Taste erfolgt eine gehende Belegung über die Chef-MULAP-Leitung. Dem Angerufenen wird die Chef-MULAP-Rufnummer im Display angezeigt.
  Standardeinstellung: Der Parameter ist aktiviert.

MULAP-Tasten nutzen

Jedem Topmitglied ist eine eigene Leitung (MULAP-Leitung) zugeordnet. Die eigene und die Leitungen aller anderen Mitglieder sind bei jedem Topmitglied als MULAP-Tasten (Leitungstasten) eingerichtet. Somit kann jedes Topmitglied alle vorhandenen MULAP-Leitungen nutzen.

Die LED einer MULAP-Taste (Leitungstaste) hat folgende Bedeutung:

- Aus: Die zugehörige Leitung ist frei und kann verwendet werden.
- Leuchtet: Die zugehörige Leitung ist belegt.

- Blinkt schnell: Anruf auf der zugehörigen Leitung.
- Blinkt langsam: Ein gehaltenes Gespräch wartet auf der zugehörigen Leitung oder die zugehörige Leitung wurde für eine Konferenz freigegeben.

Direktruftasten nutzen

Jedes Topmitglied hat für jedes andere Topmitglied eine Direktruftaste. Somit sind die Topmitglieder untereinander direkt per Tastendruck erreichbar.

Eine Direktruftaste kann auch verwendet werden, um ein bestehendes Gespräch schnell an das darunter programmierte Topmitglied zu übergeben.

Die LED einer Direktruftaste hat folgende Bedeutung:

- Aus: Das zugehörige Topmitglied telefoniert nicht.
- Leuchtet: Das zugehörige Topmitglied telefoniert oder hat Anrufschutz eingeschaltet.
- Blinkt schnell: Das zugehörige Topmitglied ruft an. Der Anruf kann durch Drücken der Direktruftaste angenommen werden.
- Blinkt langsam: Das zugehörige Topmitglied wird gerufen und hat den Anruf noch nicht angenommen. Der Anruf kann durch Drücken der Direktruftaste übernommen werden.

Rufart

Für jede Chef/Sekretär-Konfiguration/Top-Gruppe kann ein Administrator mit dem Profil **Expert** die akustische Signalisierung kommender externer Anrufe über die Einstellung der Rufart definieren. Es bestehen folgende Möglichkeiten:

- Doppel-Rufton (Standardeinstellung)
- Dreifach-Rufton
- Kurz/Lang/Kurz-Rufton

Bei analogen Telefonen ist ausschließlich die Standardeinstellung möglich. Änderungen haben keine Auswirkung.

Faxboxen für Chef/Sekretär-Konfiguration/Top-Gruppe

Für jedes Mitglied einer Chef/Sekretär-Konfiguration/Top-Gruppe kann eine Faxbox eingerichtet werden, über die das Mitglied Faxnachrichten direkt über myPortal for Desktop oder myPortal for Outlook empfangen kann.

Wurde für den ersten Chef der Chef/Sekretär-Konfiguration/Top-Gruppe bereits eine Faxbox konfiguriert, wird diese Faxbox bei der Einrichtung der Chef/Sekretär-Konfiguration/Top-Gruppe übernommen. Bereits konfigurierte Faxboxen der anderen Mitglieder werden gelöscht.

Nach dem Auflösen einer Chef/Sekretär-Konfiguration/Top-Gruppe kann nur noch der ehemalige erste Chef seine Faxbox nutzen.

SIP-Telefone

Die Einbindung von SIP-Telefonen in eine Chef/Sekretär-Konfiguration/Top-Gruppe ist möglich. Voraussetzung dafür ist, dass als erstes Mitglied (Chef 1) der Chef/Sekretär-Konfiguration/Top-Gruppe ein Systemtelefon (zum Beispiel IP-Telefon, HFA) definiert wird.

Eingebunden werden können beispielsweise Dual-Mode-Mobiltelefone, die als Mobility Entry-Teilnehmer eingerichtet sind. Dual-Mode-Mobiltelefone unterstützen sowohl GSM/UMTS-Netze als auch WLAN-Netze. Über WLAN ist die Registrierung eines Dual-Mode-Mobiltelefons als IP-Teilnehmer (SIP Client) am Kommunikationssystem möglich.

INFO: Bei SIP-Telefonen ist keine Programmierung von MULAP-Tasten und Direktruftasten möglich. Darüber hinaus können keine Leistungsmerkmale über Kennzahlen aktiviert oder deaktiviert werden. Spezifische Displaymeldungen der Chef/Sekretär-Konfiguration/Top-Gruppe werden nicht unterstützt.

Abhängigkeiten

Thema	Abhängigkeit
Anrufumleitung	Ein Topmitglied hat eine Anrufumleitung für alle Anrufe aktiviert. In diesem Fall werden alle Anrufe für seine eigene Teilnehmerrufnummer umgeleitet.
Anrufschutz	Aktiviert ein Topmitglied den Anrufschutz, werden ankommende Anrufe nicht durchgestellt.
ISDN-Telefone	Die Einbindung von ISDN-Telefonen in Chef/Sekretär-Konfigurationen/Top-Gruppen ist nicht möglich.

14.2.3 Konfiguration von Teamschaltungen / Team-Gruppen und Chef/Sekretär-Funktionen / Top-Gruppen über Wizards

Verschiedene Wizards ermöglichen die komfortable Konfiguration von Teamschaltungen (Team-Gruppen) und von Chef- und Sekretär-Funktionen (Topfunktion).

Mit dem Wizard **Teamschaltung** können Sie Teamschaltungen (Team-Gruppen) konfigurieren. Beschrieben ist die Vorgehensweise für folgende Anwendungsfälle, die über den Wizard eingerichtet werden können:

- *Wie Sie eine Teamschaltung / Team-Gruppe hinzufügen*
- *Wie Sie eine Teamschaltung / Team-Gruppe ändern*
- *Wie Sie eine Teamschaltung / Team-Gruppe löschen*

Mit dem Wizard **Chef / Sekretär** können Sie komfortable Chef- und Sekretär-Funktionen (Topfunktion) konfigurieren. Beschrieben ist die Vorgehensweise für folgende Anwendungsfälle, die über den Wizard eingerichtet werden können:

- *Wie Sie eine Chef/Sekretär- / Top-Gruppe hinzufügen*
- *Wie Sie eine Chef/Sekretär- / Top-Gruppe ändern*
- *Wie Sie eine Chef/Sekretär- / Top-Gruppe löschen*

14.2.3.1 Wie Sie eine Teamschaltung / Team-Gruppe hinzufügen

Mit dem Wizard **Teamschaltung** können Sie Teamschaltungen (Team-Gruppen) einrichten.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > User-Telefonie**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Teamschaltung** zu starten.

4) Klicken Sie auf **Hinzufügen**, um eine neue Teamschaltung einzurichten.

5) Wählen Sie in der Aufklappliste **Erstes Telefon** die Rufnummer des ersten Telefons der neuen Teamschaltung aus.

6) Klicken Sie auf **OK & Weiter**.

7) Geben Sie im Feld **Name** den Namen der neuen Teamschaltung ein, falls kein Name angezeigt wird oder eine Änderung des angezeigten Namens erforderlich ist.

Das Feld **Name** ist bereits mit dem Namen des ersten Telefons der Teamschaltung vorbelegt, falls für dieses Telefon ein Name vergeben wurde.

8) Geben Sie im Feld **Interne Rufnummer** die interne Rufnummer der neuen Teamschaltung ein, falls eine Änderung der angezeigten Rufnummer erforderlich ist.

Das Feld **Interne Rufnummer** ist bereits mit der internen Rufnummer des ersten Telefons der Teamschaltung vorbelegt.

9) Geben Sie im Feld **Durchwahlnummer** die Durchwahlnummer der neuen Teamschaltung ein, falls eine Änderung der angezeigten Durchwahlnummer erforderlich ist.

Das Feld **Durchwahlnummer** ist bereits mit der Durchwahlnummer des ersten Telefons der Teamschaltung vorbelegt.

10) Geben Sie unter **Fax** im Feld **Interne Rufnummer** die interne Rufnummer der Faxbox für die neue Teamschaltung ein, falls keine Rufnummer angezeigt wird oder eine Änderung der angezeigten Rufnummer erforderlich ist.

Das Feld **Interne Rufnummer** ist bereits mit der internen Rufnummer der Faxbox des ersten Telefons der Teamschaltung vorbelegt, falls für dieses Telefon eine Faxbox konfiguriert wurde.

11) Geben Sie unter **Fax** im Feld **Durchwahlnummer** die Durchwahlnummer der Faxbox für die neue Teamschaltung ein, falls keine Durchwahlnummer

angezeigt wird oder eine Änderung der angezeigten Durchwahlnummer erforderlich ist.

Das Feld **Durchwahlnummer** ist bereits mit der Durchwahlnummer der Faxbox des ersten Telefons der Teamschaltung vorbelegt, falls für dieses Telefon eine Faxbox konfiguriert wurde.

12) Wählen Sie in der Aufklappliste **Zweites Telefon** die Rufnummer des zweiten Telefons der neuen Teamschaltung aus.

13) Wählen Sie in der Aufklappliste **Drittes Telefon** die Rufnummer des dritten Telefons der neuen Teamschaltung aus.

14) Klicken Sie auf **OK & Weiter**.

15) Wenn Sie eine weitere Teamschaltung einrichten möchten, wiederholen Sie die Schritte 4 bis 14.

16) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

14.2.3.2 Wie Sie eine Teamschaltung / Team-Gruppe ändern

Mit dem Wizard **Teamschaltung** können Sie Teamschaltungen (Team-Gruppen) bearbeiten.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > User-Telefonie**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Teamschaltung** zu starten.

4) Klicken Sie in der Zeile der zu ändernden Teamschaltung auf **Bearbeiten**.

5) Ändern Sie die gewünschten Parameter.

6) Nur bei UC Smart: Ordnen Sie bei Bedarf der Teamschaltung eine Mailbox zu:

a) Wählen Sie in der Aufklappliste **Mailboxtyp UC Smart** aus, ob die Teamschaltung eine Standardmailbox oder eine Vermittlungsmailbox (AutoAttendant) erhalten soll.

b) Nur bei Standardmailbox: Wenn ein Anrufer eine Nachricht auf der Sprachbox hinterlassen darf, aktivieren Sie das Kontrollkästchen **Aufnahme**.

c) Wählen Sie aus der Aufklappliste **Begrüßung** eine Begrüßung aus.

d) Wenn das Kennwort der Sprachbox zurückgesetzt werden soll, aktivieren Sie das Kontrollkästchen **Passwort Reset**.

INFO: Das Kontrollkästchen **Passwort Reset** muss bei einer Neueinrichtung einer Sprachbox nicht gesetzt sein. Es bewirkt

das Rücksetzen des Kennworts der Sprachbox. Bei einer Neueinrichtung muss der Teilnehmer sowieso beim ersten Zugriff auf seine Sprachbox das Initial-Kennwort ändern.

7) Klicken Sie auf **OK & Weiter**.

8) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

14.2.3.3 Wie Sie eine Teamschaltung / Team-Gruppe löschen

Mit dem Wizard **Teamschaltung** können Sie Teamschaltungen (Team-Gruppen) löschen.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > User-Telefonie**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Teamschaltung** zu starten.

4) Klicken Sie in der Zeile der zu löschenden Teamschaltung auf **Bearbeiten**.

5) Klicken Sie auf **Daten löschen**.

6) Klicken Sie auf **OK**, um das Löschen zu bestätigen.

7) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

14.2.3.4 Wie Sie eine Chef/Sekretär- / Top-Gruppe hinzufügen

Mit dem Wizard **Chef / Sekretär** können Sie komfortable Chef- und Sekretär-Funktionen (Topfunktion) einrichten.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > User-Telefonie**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Chef / Sekretär** zu starten.

4) Klicken Sie auf **Hinzufügen**, um eine neue Chef/Sekretär-Konfiguration (Top-Gruppe) einzurichten.

5) Geben Sie im Feld **Name** den Namen der neuen Chef/Sekretär-Konfiguration ein.

6) Wählen Sie in den zugehörigen Aufklapplisten die gewünschten Rufnummern der neuen Chef/Sekretär-Konfiguration aus.

7) Klicken Sie auf **OK & Weiter**.

8) Geben Sie unter **Fax** im Feld **Rufnummer** die interne Rufnummer der Faxbox für die neue Chef/Sekretär-Konfiguration ein, falls keine Rufnummer angezeigt wird oder eine Änderung der angezeigten Rufnummer erforderlich ist.

Das Feld **Rufnummer** ist bereits mit der internen Rufnummer der Faxbox des ersten Chefs der Chef/Sekretär-Konfiguration vorbelegt, falls für dieses Telefon eine Faxbox konfiguriert wurde.

9) Geben Sie unter **Fax** im Feld **Durchwahl** die Durchwahlnummer der Faxbox für die neue Chef/Sekretär-Konfiguration ein, falls keine Durchwahlnummer angezeigt wird oder eine Änderung der angezeigten Durchwahlnummer erforderlich ist.

Das Feld **Durchwahl** ist bereits mit der Durchwahlnummer der Faxbox des ersten Chefs der Chef/Sekretär-Konfiguration vorbelegt, falls für dieses Telefon eine Faxbox konfiguriert wurde.

10) Wählen Sie eine Vorgabe für die Tastenbelegung aus:

- Wenn die Tasten für die Chef/Sekretär-Funktionen auf dem ersten oder zweiten Beistellgerät eingerichtet werden sollen, aktivieren Sie das Kontrollkästchen **auf erste/zweite Konsole**.
- Wenn die Tasten für die Chef/Sekretär-Funktionen auf den ersten freien Funktionstasten des Telefons eingerichtet werden sollen, aktivieren Sie das Kontrollkästchen **auf erste freie Tasten**.

11) Klicken Sie auf **OK & Weiter**.

12) Wenn Sie eine weitere Chef/Sekretär-Konfiguration einrichten möchten, wiederholen Sie die Schritte 4 bis 11.

13) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

14.2.3.5 Wie Sie eine Chef/Sekretär- / Top-Gruppe ändern

Mit dem Wizard **Chef / Sekretär** können Sie komfortable Chef- und Sekretär-Funktionen (Topfunktion) bearbeiten.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > User-Telefonie**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Chef / Sekretär** zu starten.

4) Klicken Sie in der Zeile der zu ändernden Chef/Sekretär-Konfiguration (Top-Gruppe) auf **Bearbeiten**.

5) Ändern Sie die gewünschten Parameter.

6) Nur bei UC Smart: Ordnen Sie bei Bedarf der Top-Gruppe eine Mailbox zu:

a) Wählen Sie in der Aufklappliste **Mailboxtyp UC Smart** aus, ob die Top-Gruppe eine Standardmailbox oder eine Vermittlungsmailbox (AutoAttendant) erhalten soll.

b) Nur bei Standardmailbox: Wenn ein Anrufer eine Nachricht auf der Sprachbox hinterlassen darf, aktivieren Sie das Kontrollkästchen **Aufnahme**.

c) Wählen Sie aus der Aufklappliste **Begrüßung** eine Begrüßung aus.

d) Wenn das Kennwort der Sprachbox zurückgesetzt werden soll, aktivieren Sie das Kontrollkästchen **Passwort Reset**.

INFO: Das Kontrollkästchen **Passwort Reset** muss bei einer Neueinrichtung einer Sprachbox nicht gesetzt sein. Es bewirkt das Rücksetzen des Kennworts der Sprachbox. Bei einer Neueinrichtung muss der Teilnehmer sowieso beim ersten Zugriff auf seine Sprachbox das Initial-Kennwort ändern.

---

7) Klicken Sie auf **OK & Weiter**.

8) Ändern Sie die gewünschten Angaben für die Faxbox (**Fax**) und die **Tastenvergabe**.

9) Klicken Sie auf **OK & Weiter**.

10) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

14.2.3.6 Wie Sie eine Chef/Sekretär- / Top-Gruppe löschen

Mit dem Wizard **Chef / Sekretär** können Sie komfortable Chef- und Sekretär-Funktionen (Topfunktion) löschen.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > User-Telefonie**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Chef / Sekretär** zu starten.

4) Klicken Sie in der Zeile der zu löschenden Chef/Sekretär-Konfiguration (Top-Gruppe) auf **Bearbeiten**.

5) Klicken Sie auf **Daten löschen**.

6) Klicken Sie auf **OK**, um das Löschen zu bestätigen.

7) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

14.2.4 Konfiguration von Teamschaltungen / Team-Gruppen und Chef/ Sekretär-Funktionen / Top-Gruppen über Experten-Modus

Neben den Konfigurationsmöglichkeiten über Wizards stehen einem Administrator mit dem Profil **Expert** zusätzliche Möglichkeiten zur Konfiguration von Teamschaltungen / Team-Gruppen und Chef/Sekretär-Funktionen / Top-Gruppen über den **Experten-Modus** zur Verfügung.

Beschrieben ist die Vorgehensweise für folgende Anwendungsfälle, die über den **Experten-Modus** eingerichtet werden können:

- *Wie Sie ein Mitglied zur Teamschaltung / Team-Gruppe hinzufügen oder löschen*
- *Wie Sie ein Mitglied einer Teamschaltung / Team-Gruppe ändern*
- *Wie Sie die Eigenschaften der Mitglieder einer Teamschaltung / Team-Gruppe ändern*
- *Wie Sie die Telefon-Tastenbelegung für Teamschaltung / Team-Gruppe ändern*
- *Wie Sie eine Faxbox zur Teamschaltung / Team-Gruppe hinzufügen*
- *Wie Sie ein Mitglied zur Chef/Sekretär / Top-Gruppe hinzufügen oder löschen*
- *Wie Sie ein Mitglied einer Chef/Sekretär / Top-Gruppe ändern*
- *Wie Sie die Eigenschaften der Mitglieder einer Chef/Sekretär / Top-Gruppe ändern*
- *Wie Sie eine Faxbox zur Chef/Sekretär / Top-Gruppe hinzufügen*

14.2.4.1 Wie Sie ein Mitglied zur Teamschaltung / Team-Gruppe hinzufügen oder löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

> ***INFO:*** Mit dem Wizard **Teamschaltung** kann ein Administrator mit dem Profil **Advanced** bis zu drei Mitglieder (Telefone) für eine Teamschaltung (Team-Gruppe) definieren. Zusätzliche Mitglieder muss ein Administrator mit dem Profil **Expert** über den **Experten-Modus** hinzufügen (siehe folgende Beschreibung).

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Kommende Rufe**.

3) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie ein Mitglied zur Team-Gruppe (Teamschaltung) hinzufügen möchten, navigieren Sie im Menübaum unter **Kommende Rufe > Team/ Top > …** zur gewünschten Team-Gruppe (Teamschaltung). Klicken Sie auf die Registerkarte **Team/Top Mitglied hinzufügen**. Wählen Sie in der Aufklappliste **Typ** den Teilnehmer-Typ aus. Wählen Sie in der Aufklappliste **Ruf-Nr.** die Rufnummer des gewünschten Teilnehmers aus. Klicken Sie auf **Übernehmen** und anschließend auf **OK**.
- Wenn Sie ein Mitglied aus der Team-Gruppe (Teamschaltung) entfernen möchten, navigieren Sie im Menübaum unter **Kommende Rufe > Team/ Top > …** zum gewünschten Mitglied der Team-Gruppe (Teamschaltung) ((Gruppenmitglied) Rufnummer Name). Klicken Sie auf die Registerkarte **Team/Top Mitglied löschen**. Klicken Sie auf **Löschen** und anschließend auf **OK**.

14.2.4.2 Wie Sie ein Mitglied einer Teamschaltung / Team-Gruppe ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Kommende Rufe**.

3) Navigieren Sie im Menübaum unter **Kommende Rufe > Team/Top > …** zum gewünschten Mitglied der Team-Gruppe (Teamschaltung) ((Gruppenmitglied) Rufnummer Name).

4) Klicken Sie auf die Registerkarte **Team/Top Mitglied ändern**.

5) Ändern Sie die gewünschten Parameter.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

14.2.4.3 Wie Sie die Eigenschaften der Mitglieder einer Teamschaltung / Team-Gruppe ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Kommende Rufe**.

3) Navigieren Sie im Menübaum unter **Kommende Rufe > Team/Top > …** zu einem Mitglied der Team-Gruppe (Teamschaltung) ((Gruppenmitglied) Rufnummer Name).

4) Klicken Sie auf die Registerkarte **Team/Top Gruppen-Parameter ändern**.

5) Ändern Sie die gewünschten Eigenschaften.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

14.2.4.4 Wie Sie die Telefon-Tastenbelegung für Teamschaltung / Team-Gruppe ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Kommende Rufe**.

3) Navigieren Sie im Menübaum unter **Kommende Rufe > Team/Top > …** zur gewünschten Team-Gruppe (Teamschaltung).

4) Klicken Sie auf die Registerkarte **Team/Top Gruppe ändern**.

5) Wählen Sie eine Vorgabe für die Tastenbelegung aus:

- Wenn die Tasten auf dem ersten oder zweiten Beistellgerät eingerichtet werden sollen, aktivieren Sie das Kontrollkästchen **auf erste /zweite Konsole**.
- Wenn die Tasten auf den ersten freien Funktionstasten des Telefons eingerichtet werden sollen, aktivieren Sie das Kontrollkästchen **auf erste freie Tasten**.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

14.2.4.5 Wie Sie eine Faxbox zur Teamschaltung / Team-Gruppe hinzufügen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Kommende Rufe**.

3) Navigieren Sie im Menübaum unter **Kommende Rufe > Team/Top > …** zur gewünschten Team-Gruppe (Teamschaltung).

4) Klicken Sie auf die Registerkarte **Fax Box hinzufügen**.

5) Geben Sie im Feld **Fax Rufnr.** des gewünschten Mitglieds der Team-Gruppe (Teamschaltung) die interne Rufnummer der Faxbox ein.

6) Geben Sie im Feld **Fax DuWa** des gewünschten Mitglieds der Team-Gruppe (Teamschaltung) die Durchwahlnummer der Faxbox ein.

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

14.2.4.6 Wie Sie ein Mitglied zur Chef/Sekretär / Top-Gruppe hinzufügen oder löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

INFO: Mit dem Wizard **Chef / Sekretär** kann ein Administrator mit dem Profil **Advanced** bis zu zwei Chefs und bis zu zwei Sekretäre pro Chef/Sekretär-Konfiguration (Top-Gruppe) definieren. Zusätzliche Mitglieder muss ein Administrator mit dem Profil **Expert** über den **Experten-Modus** hinzufügen (siehe folgende Beschreibung).

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Kommende Rufe**.

3) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie ein Mitglied zur Top-Gruppe (Chef/Sekretär-Konfiguration) hinzufügen möchten, navigieren Sie im Menübaum unter **Kommende Rufe > Team/Top > …** zur gewünschten Top-Gruppe (Chef/Sekretär-Konfiguration). Klicken Sie auf die Registerkarte **Team/Top Mitglied hinzufügen**. Wählen Sie in der Aufklappliste **Typ** den Teilnehmer-Typ aus. Wählen Sie in der Aufklappliste **Ruf-Nr.** die Rufnummer des gewünschten Teilnehmers aus. Klicken Sie auf **Übernehmen** und anschließend auf **OK**.
- Wenn Sie ein Mitglied aus der Top-Gruppe (Chef/Sekretär-Konfiguration) entfernen möchten, navigieren Sie im Menübaum unter **Kommende Rufe > Team/Top > …** zum gewünschten Mitglied der Top-Gruppe (Chef/Sekretär-Konfiguration) ((Gruppenmitglied) Rufnummer Name). Klicken Sie auf die Registerkarte **Team/Top Mitglied löschen**. Klicken Sie auf **Löschen** und anschließend auf **OK**.

14.2.4.7 Wie Sie ein Mitglied einer Chef/Sekretär / Top-Gruppe ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Kommende Rufe**.
3) Navigieren Sie im Menübaum unter **Kommende Rufe > Team/Top > …** zum gewünschten Mitglied der Top-Gruppe (Chef/Sekretär-Konfiguration) ((Gruppenmitglied) Rufnummer Name).
4) Klicken Sie auf die Registerkarte **Team/Top Mitglied ändern**.
5) Ändern Sie die gewünschten Parameter.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

14.2.4.8 Wie Sie die Eigenschaften der Mitglieder einer Chef/Sekretär / Top-Gruppe ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Kommende Rufe**.
3) Navigieren Sie im Menübaum unter **Kommende Rufe > Team/Top > …** zu einem Mitglied der Top-Gruppe (Chef/Sekretär-Konfiguration) ((Gruppenmitglied) Rufnummer Name).
4) Klicken Sie auf die Registerkarte **Team/Top Gruppen-Parameter ändern**.
5) Ändern Sie die gewünschten Eigenschaften.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

14.2.4.9 Wie Sie eine Faxbox zur Chef/Sekretär / Top-Gruppe hinzufügen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Kommende Rufe**.
3) Navigieren Sie im Menübaum unter **Kommende Rufe > Team/Top > …** zur gewünschten Top-Gruppe (Chef/Sekretär-Konfiguration).
4) Klicken Sie auf die Registerkarte **Fax Box hinzufügen**.

5) Geben Sie im Feld **Fax Rufnr.** des gewünschten Mitglieds der Top-Gruppe (Chef/Sekretär-Konfiguration) die interne Rufnummer der Faxbox ein.

6) Geben Sie im Feld **Fax DuWa** des gewünschten Mitglieds der Top-Gruppe (Chef/Sekretär-Konfiguration) die Durchwahlnummer der Faxbox ein.

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

14.3 Basic-MULAP und Chef-MULAP

Eine Basic-MULAP ermöglicht einem Teilnehmer, der mehrere Telefone (zum Beispiel Festnetztelefon und Mobiltelefon) nutzt, unter einer Rufnummer erreichbar zu sein. Chef-MULAPs können eingerichtet werden, wenn eingeschränkte Chef- und Sekretär-Funktionen genutzt werden sollen.

14.3.1 Basic-MULAP

Basic-MULAPs können eingerichtet werden, wenn ein Teilnehmer mehrere Telefone (zum Beispiel Festnetztelefon und Mobiltelefon) nutzt, aber unter einer Rufnummer (Basic-MULAP-Rufnummer) erreichbar sein möchte.

Wählt ein Anrufer die Basic-MULAP-Rufnummer, wird der Anruf bei allen zur Basic-MULAP gehörenden Telefonen optisch signalisiert. Für jedes Mitglied kann zusätzlich angegeben werden, ob ankommende Anrufe auch akustisch signalisiert werden sollen. Nach Annahme des Anrufs ist die Basic-MULAP besetzt und weitere Anrufer erhalten den Besetztton.

Bei gehenden Anrufen über die Basic-MULAP-Leitung wird den Angerufenen die Basic-MULAP-Rufnummer im Display angezeigt.

Bis zu 20 Mitglieder pro Basic-MULAP können eingerichtet werden.

Jeder Basic-MULAP kann ein maximal 16 Zeichen langer Name zugewiesen werden.

Jedes Telefon des Teilnehmers wird Mitglied der Basic-MULAP, wobei den Mitgliedern folgende Eigenschaften zugewiesen werden können:

- **Master**
  Durch diesen Parameter wird ein Mitglied zu einem Master der Basic-MULAP. Aktiviert ein Master eine Anrufumleitung, gilt diese für alle Mitglieder (Telefone) der Basic-MULAP. Nach Aktivierung eines automatischen Rückrufs auf eine Basic-MULAP, wird der Rückruf eingeleitet, sobald alle Master frei sind.
  Ein Teilnehmer darf als MULAP-Master in Sammelanschlüssen nicht mehr als 25 mal aufgenommen werden.
  Standardeinstellung: Master ist das erste Mitglied der Basic-MULAP.
- **Akustischer Ruf**
  Ist dieser Parameter aktiviert, werden ankommende Anrufe akustisch signalisiert.
  Standardeinstellung: Der Parameter ist bei allen Mastern aktiviert.

- **Automatische Belegung gehend**
  Ist dieser Parameter aktiviert, wird beim Abheben des Hörers automatisch über die Basic-MULAP-Leitung gerufen. Bei nicht aktiviertem Parameter muss der Teilnehmer die MULAP-Taste betätigen, bevor er wählen kann.
  Standardeinstellung: Die automatische Belegung gehend erhalten alle Master.
- **Keine automatische Rufannahme kommend**
  Ist dieser Parameter aktiviert, kann ein kommender Anruf nicht durch Abheben des Hörers angenommen werden. Ein kommender Anruf muss durch Betätigen der MULAP-Taste angenommen werden.
  Standardeinstellung: Der Parameter ist nicht aktiviert.
- **Automatische Konferenzfreigabe**
  Bei aktiviertem Parameter wird durch Drücken der MULAP-Taste die belegte MULAP-Leitung für eine Konferenz freigegeben. Bei allen weiteren Mitgliedern wird die Freigabe durch Blinken der MULAP-Taste angezeigt. Durch das Drücken der MULAP-Taste können sie sich in die Konferenz hineinschalten.
  Standardeinstellung: Der Parameter ist nicht aktiviert.
- **MULAP-Taste eingerichtet**
  Bei aktiviertem Parameter wird bei dem zugehörigen Telefon eine MULAP-Taste eingerichtet. Durch Drücken der Taste erfolgt eine gehende Belegung über die Basic-MULAP-Leitung. Dem Angerufenen wird die Basic-MULAP-Rufnummer im Display angezeigt.
  Standardeinstellung: Der Parameter ist aktiviert.

MULAP-Tasten nutzen

Die LED einer MULAP-Taste hat folgende Bedeutung:

- Aus: Die zugehörige Leitung ist frei und kann verwendet werden.
- Leuchtet: Die zugehörige Leitung ist belegt.
- Blinkt schnell: Anruf auf der zugehörigen Leitung.
- Blinkt langsam: Ein gehaltenes Gespräch wartet auf der zugehörigen Leitung oder die zugehörige Leitung wurde für eine Konferenz freigegeben.

Rufart

Für jede Basic-MULAP kann ein Administrator mit dem Profil **Expert** die akustische Signalisierung kommender externer Anrufe über die Einstellung der Rufart definieren. Es bestehen folgende Möglichkeiten:

- Doppel-Rufton (Standardeinstellung)
- Dreifach-Rufton
- Kurz/Lang/Kurz-Rufton

Bei analogen Telefonen ist ausschließlich die Standardeinstellung möglich. Änderungen haben keine Auswirkung.

SIP-Telefone

Die Einbindung von SIP-Telefonen in eine Basic-MULAP ist möglich. Voraussetzung dafür ist, dass als erstes Mitglied der Basic-MULAP ein Systemtelefon (zum Beispiel IP-Telefon, HFA) definiert wird.

Eingebunden werden können beispielsweise Dual-Mode-Mobiltelefone, die als Mobility Entry-Teilnehmer eingerichtet sind. Dual-Mode-Mobiltelefone unterstützen sowohl GSM/UMTS-Netze als auch WLAN-Netze. Über WLAN ist die Registrierung eines Dual-Mode-Mobiltelefons als IP-Teilnehmer (SIP Client) am Kommunikationssystem möglich.

INFO: Bei SIP-Telefonen ist keine Programmierung von MULAP-Tasten möglich. Darüber hinaus können keine Leistungsmerkmale über Kennzahlen aktiviert oder deaktiviert werden. Spezifische Displaymeldungen der Basic-MULAP werden nicht unterstützt.

Abhängigkeiten

Thema	Abhängigkeit
Anrufschutz	Nach Aktivierung des Anrufschutzes, werden ankommende Anrufe nicht durchgestellt.
ISDN-Telefone	Die Einbindung von ISDN-Telefonen in Basic-MULAPs ist nicht möglich.

Verwandte Themen

- Wie Sie Basic-MULAP hinzufügen
- Wie Sie Basic-MULAP anzeigen oder ändern
- Wie Sie Basic-MULAP löschen
- Wie Sie ein Mitglied zur Basic-MULAP hinzufügen oder löschen
- Wie Sie ein Mitglied einer Basic-MULAP ändern

14.3.2 Chef-MULAP

Chef-MULAPs können eingerichtet werden, wenn eingeschränkte Chef- und Sekretär-Funktionen genutzt werden sollen.

Alle Mitglieder einer Chef-MULAP sind unter der Chef-MULAP-Rufnummer und unter ihren eigenen Teilnehmerrufnummern erreichbar.

INFO: In diesem Text steht "der Chef” stellvertretend sowohl für Chef als auch Chefin und “der Sekretär” stellvertretend sowohl für Sekretär als auch Sekretärin.

Bis zu 20 Mitglieder pro Chef-MULAP können eingerichtet werden.

Jeder Chef-MULAP kann ein maximal 16 Zeichen langer Name zugewiesen werden.

Über die nachfolgend beschriebenen Parameter wird definiert, welche Mitglieder einer Chef-MULAP Chef-Funktionen (Chef) und welche Sekretär-Funktionen (Sekretär) nutzen können.

Wählt ein Anrufer die Chef-MULAP-Rufnummer, wird der Anruf bei allen zur Chef-MULAP gehörenden Telefonen optisch signalisiert. Bei Mitgliedern mit Sekretär-Funktionen werden ankommende Anrufe auch akustisch signalisiert.

Bei gehenden Anrufen über die Chef-MULAP-Leitung wird den Angerufenen die Chef-MULAP-Rufnummer im Display angezeigt.

Den Mitgliedern einer Chef-MULAP können folgende Eigenschaften zugewiesen werden:

- **Master**
  Durch diesen Parameter werden einem Mitglied Chef-Funktionen zugewiesen. Beim Abheben des Hörers wird automatisch über die Chef-MULAP-Leitung gerufen. Ankommende Anrufe über Chef-MULAP-Rufnummer werden ausschließlich optisch signalisiert.
  Ein Teilnehmer darf als MULAP-Master in Sammelanschlüssen nicht mehr als 25 mal aufgenommen werden.
  Standardeinstellung: Chef-Funktionen erhält das erste Mitglied der Chef-MULAP.
- **Akustischer Ruf**
  Ist dieser Parameter aktiviert, werden ankommende Anrufe akustisch signalisiert.
  Standardeinstellung: Der Parameter ist für alle Mitglieder mit Sekretär-Funktion aktiviert.
- **Automatische Belegung gehend**
  Ist dieser Parameter aktiviert, wird beim Abheben des Hörers automatisch über die Chef-MULAP-Leitung gerufen. Bei nicht aktiviertem Parameter muss der Teilnehmer die MULAP-Taste betätigen, bevor er wählen kann.
  Dieser Parameter kann nicht von Mitgliedern mit Sekretär-Funktion genutzt werden.
  Standardeinstellung: Der Parameter ist für alle Mitglieder mit Chef-Funktion aktiviert.
- **Keine automatische Rufannahme kommend**
  Ist dieser Parameter aktiviert, kann ein kommender Anruf nicht durch Abheben des Hörers angenommen werden. Ein kommender Anruf muss durch Betätigen der MULAP-Taste angenommen werden.
  Standardeinstellung: Der Parameter ist nicht aktiviert.
- **Automatische Konferenzfreigabe**
  Bei aktiviertem Parameter wird durch Drücken der MULAP-Taste die belegte MULAP-Leitung für eine Konferenz freigegeben. Bei allen weiteren Mitgliedern wird die Freigabe durch Blinken der MULAP-Taste angezeigt. Durch das Drücken der MULAP-Taste können sie sich in die Konferenz hineinschalten.
  Standardeinstellung: Der Parameter ist nicht aktiviert.

- **MULAP-Taste eingerichtet**
  Bei aktiviertem Parameter wird bei dem zugehörigen Telefon eine MULAP-Taste eingerichtet. Durch Drücken der Taste erfolgt eine gehende Belegung über die Chef-MULAP-Leitung. Dem Angerufenen wird die Chef-MULAP-Rufnummer im Display angezeigt.
  Standardeinstellung: Der Parameter ist aktiviert.

MULAP-Tasten nutzen

Die LED einer MULAP-Taste hat folgende Bedeutung:

- Aus: Die zugehörige Leitung ist frei und kann verwendet werden.
- Leuchtet: Die zugehörige Leitung ist belegt.
- Blinkt schnell: Anruf auf der zugehörigen Leitung.
- Blinkt langsam: Ein gehaltenes Gespräch wartet auf der zugehörigen Leitung oder die zugehörige Leitung wurde für eine Konferenz freigegeben.

Rufart

Für jede Chef-MULAP kann ein Administrator mit dem Profil **Expert** die akustische Signalisierung kommender externer Anrufe über die Einstellung der Rufart definieren. Es bestehen folgende Möglichkeiten:

- Doppel-Rufton (Standardeinstellung)
- Dreifach-Rufton
- Kurz/Lang/Kurz-Rufton

Bei analogen Telefonen ist ausschließlich die Standardeinstellung möglich. Änderungen haben keine Auswirkung.

SIP-Telefone

Die Einbindung von SIP-Telefonen in eine Chef-MULAP ist möglich. Voraussetzung dafür ist, dass als erstes Mitglied der Chef-MULAP (Chef 1) ein Systemtelefon (zum Beispiel IP-Telefon, HFA) definiert wird.

Eingebunden werden können beispielsweise Dual-Mode-Mobiltelefone, die als Mobility Entry-Teilnehmer eingerichtet sind. Dual-Mode-Mobiltelefone unterstützen sowohl GSM/UMTS-Netze als auch WLAN-Netze. Über WLAN ist die Registrierung eines Dual-Mode-Mobiltelefons als IP-Teilnehmer (SIP Client) am Kommunikationssystem möglich.

> ***INFO:*** Bei SIP-Telefonen ist keine Programmierung von MULAP-Tasten möglich. Darüber hinaus können keine Leistungsmerkmale über Kennzahlen aktiviert oder deaktiviert werden. Spezifische Displaymeldungen der Chef-MULAP werden nicht unterstützt.

Abhängigkeiten

Thema	Abhängigkeit
Anrufschutz	Nach Aktivierung des Anrufschutzes, werden ankommende Anrufe nicht durchgestellt.
ISDN-Telefone	Die Einbindung von ISDN-Telefonen in Chef-MULAPs ist nicht möglich.

Verwandte Themen

- Wie Sie eine Chef-MULAP hinzufügen
- Wie Sie eine Chef-MULAP anzeigen oder ändern
- Wie Sie eine Chef-MULAP löschen
- Wie Sie ein Mitglied zur Chef-MULAP hinzufügen oder löschen
- Wie Sie ein Mitglied einer Chef-MULAP ändern

14.3.3 Konfiguration von Basic-MULAPs und Chef-MULAPs

Die Konfiguration von Basic-MULAPs und von Chef-MULAPs ist ausschließlich durch einen Administrator mit dem Profil **Expert** über den **Experten-Modus** möglich.

Beschrieben ist die Vorgehensweise für folgende Anwendungsfälle, die über den **Experten-Modus** eingerichtet werden können:

- *Wie Sie Basic-MULAP hinzufügen*
- *Wie Sie Basic-MULAP anzeigen oder ändern*
- *Wie Sie Basic-MULAP löschen*
- *Wie Sie ein Mitglied zur Basic-MULAP hinzufügen oder löschen*
- *Wie Sie ein Mitglied einer Basic-MULAP ändern*
- *Wie Sie eine Chef-MULAP hinzufügen*
- *Wie Sie eine Chef-MULAP anzeigen oder ändern*
- *Wie Sie eine Chef-MULAP löschen*
- *Wie Sie ein Mitglied zur Chef-MULAP hinzufügen oder löschen*
- *Wie Sie ein Mitglied einer Chef-MULAP ändern*

14.3.3.1 Wie Sie Basic-MULAP hinzufügen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Kommende Rufe**.
3) Klicken Sie im Menübaum auf **Kommende Rufe > Gruppen-/Sammelanschluss**.
4) Klicken Sie auf die Registerkarte **Gruppe hinzufügen**.
5) Geben Sie im Feld **Rufnummer** die Rufnummer der neuen Basic-MULAP ein.
6) Geben Sie im Feld **Durchwahlnummer** die Durchwahlnummer der neuen Basic-MULAP ein.
7) Geben Sie im Feld **Name** den Namen der neuen Basic-MULAP ein.
8) Wählen Sie in der Aufklappliste **Typ** den Eintrag **Basic-MULAP** aus.
9) Wählen Sie in der Aufklappliste **Rufnummer** die Rufnummer des Teilnehmers aus, der der Basic-MULAP zugeordnet werden soll.
10) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Verwandte Themen

- Basic-MULAP

14.3.3.2 Wie Sie Basic-MULAP anzeigen oder ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Kommende Rufe**.
3) Navigieren Sie im Menübaum unter **Kommende Rufe > Gruppen-/Sammelanschluss > …** zur gewünschten Basic-MULAP.
4) Klicken Sie auf die Registerkarte **Gruppen-Parameter ändern**. Ihnen werden die aktuellen Einstellungen der Gruppen-Parameter angezeigt.
5) Ändern Sie bei Bedarf die gewünschten Parameter der Basic-MULAP.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Verwandte Themen

- Basic-MULAP

14.3.3.3 Wie Sie Basic-MULAP löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Kommende Rufe**.
3) Navigieren Sie im Menübaum unter **Kommende Rufe > Gruppen-/Sammelanschluss > …** zur gewünschten Basic-MULAP.
4) Klicken Sie auf die Registerkarte **Gruppe löschen**.
5) Klicken Sie auf **Löschen** und anschließend auf **OK**.

Verwandte Themen

- Basic-MULAP

14.3.3.4 Wie Sie ein Mitglied zur Basic-MULAP hinzufügen oder löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Kommende Rufe**.
3) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie ein Mitglied zur Basic-MULAP hinzufügen möchten, navigieren Sie im Menübaum unter **Kommende Rufe > Gruppen-/Sammelanschluss > …** zur gewünschten Basic-MULAP. Klicken Sie auf die Registerkarte **Mitglied hinzufügen**. Wählen Sie in der Aufklappliste **Rufnummer** die Rufnummer des gewünschten Teilnehmers aus. Klicken Sie auf **Übernehmen** und anschließend auf **OK**.
   - Wenn Sie ein Mitglied aus der Basic-MULAP entfernen möchten, navigieren Sie im Menübaum unter **Kommende Rufe > Gruppen-/Sammelanschluss > …** zum gewünschten Mitglied der Basic-MULAP ((Gruppenmitglied) Rufnummer Name). Klicken Sie auf die Registerkarte **Mitglied löschen**. Klicken Sie auf **Löschen** und anschließend auf **OK**.

Verwandte Themen

- Basic-MULAP

14.3.3.5 Wie Sie ein Mitglied einer Basic-MULAP ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Kommende Rufe**.

3) Navigieren Sie im Menübaum unter **Kommende Rufe > Gruppen-/Sammelanschluss > …** zum gewünschten Mitglied der Basic-MULAP ((Gruppenmitglied) Rufnummer Name).

4) Klicken Sie auf die Registerkarte **Mitglied ändern**.

5) Ändern Sie die gewünschten Parameter.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Verwandte Themen

- Basic-MULAP

14.3.3.6 Wie Sie eine Chef-MULAP hinzufügen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Kommende Rufe**.

3) Klicken Sie im Menübaum auf **Kommende Rufe > Gruppen-/Sammelanschluss**.

4) Klicken Sie auf die Registerkarte **Gruppe hinzufügen**.

5) Geben Sie im Feld **Rufnummer** die Rufnummer der neuen Chef-MULAP ein.

6) Geben Sie im Feld **Durchwahlnummer** die Durchwahlnummer der neuen Chef-MULAP ein.

7) Geben Sie im Feld **Name** den Namen der neuen Chef-MULAP ein.

8) Wählen Sie in der Aufklappliste **Typ** den Eintrag **Chef-MULAP** aus.

9) Wählen Sie in der Aufklappliste **Rufnummer** die Rufnummer des Teilnehmers aus, der der Chef-MULAP zugeordnet werden soll.

10) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Verwandte Themen

- Chef-MULAP

14.3.3.7 Wie Sie eine Chef-MULAP anzeigen oder ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Kommende Rufe**.

3) Navigieren Sie im Menübaum unter **Kommende Rufe > Gruppen-/Sammelanschluss > …** zur gewünschten Chef-MULAP.

4) Klicken Sie auf die Registerkarte **Gruppen-Parameter ändern**. Ihnen werden die aktuellen Einstellungen der Gruppen-Parameter angezeigt.

5) Ändern Sie bei Bedarf die gewünschten Parameter der Chef-MULAP.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Verwandte Themen

- Chef-MULAP

14.3.3.8 Wie Sie eine Chef-MULAP löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Kommende Rufe**.

3) Navigieren Sie im Menübaum unter **Kommende Rufe > Gruppen-/Sammelanschluss > …** zur gewünschten Chef-MULAP.

4) Klicken Sie auf die Registerkarte **Gruppe löschen**.

5) Klicken Sie auf **Löschen** und anschließend auf **OK**.

Verwandte Themen

- Chef-MULAP

14.3.3.9 Wie Sie ein Mitglied zur Chef-MULAP hinzufügen oder löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Kommende Rufe**.

3) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie ein Mitglied zur Chef-MULAP hinzufügen möchten, navigieren Sie im Menübaum unter **Kommende Rufe > Gruppen-/Sammelanschluss > …** zur gewünschten Chef-MULAP. Klicken Sie auf die Registerkarte **Mitglied hinzufügen**. Wählen Sie in der Aufklappliste **Rufnummer** die Rufnummer des gewünschten Teilnehmers aus. Klicken Sie auf **Übernehmen** und anschließend auf **OK**.
- Wenn Sie ein Mitglied aus der Chef-MULAP entfernen möchten, navigieren Sie im Menübaum unter **Kommende Rufe > Gruppen-/Sammelanschluss > …** zum gewünschten Mitglied der Chef-MULAP ((Gruppenmitglied) Rufnummer Name). Klicken Sie auf die Registerkarte **Mitglied löschen**. Klicken Sie auf **Löschen** und anschließend auf **OK**.

Verwandte Themen

- Chef-MULAP

14.3.3.10 Wie Sie ein Mitglied einer Chef-MULAP ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Kommende Rufe**.

3) Navigieren Sie im Menübaum unter **Kommende Rufe > Gruppen-/Sammelanschluss > …** zum gewünschten Mitglied der Chef-MULAP ((Gruppenmitglied) Rufnummer Name).

4) Klicken Sie auf die Registerkarte **Mitglied ändern**.

5) Ändern Sie die gewünschten Parameter.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Verwandte Themen

- Chef-MULAP

14.4 Sprachbox-Gruppe und Faxbox-Gruppe

Durch eine Sprachbox-Gruppe (Anrufbeantworter-Gruppe) kann einer Teilnehmergruppe der Zugriff auf Sprachnachrichten ermöglicht werden. Über die Rufnummer der Sprachbox-Gruppe werden nicht die Mitglieder dieser Gruppe gerufen, sondern wird direkt die Sprachbox (der Anrufbeantworter) der Gruppe erreicht. Durch eine Faxbox-Gruppe (Faxgruppe) kann einer Teilnehmergruppe der Zugriff auf Faxnachrichten ermöglicht werden. Über die Rufnummer der Faxbox-Gruppe wird direkt die Faxbox der Gruppe erreicht.

14.4.1 Sprachbox-Gruppe

Durch eine Sprachbox-Gruppe (Anrufbeantworter-Gruppe) kann einer bestimmten Gruppe von Teilnehmern der Zugriff auf Sprachnachrichten ermöglicht werden. Über die Rufnummer der Sprachbox-Gruppe werden nicht die Mitglieder dieser Gruppe gerufen, sondern wird direkt die Sprachbox (der Anrufbeantworter) der Gruppe erreicht. Nachdem eine Sprachnachricht auf der Sprachbox der Gruppe hinterlassen wurde, erfolgt eine Weiterleitung an die Sprachboxen aller Mitglieder.

Alle Mitglieder erhalten die Sprachnachricht gleichzeitig. Löscht ein Mitglied der Gruppe eine Sprachnachricht, wird diese auch aus den Sprachboxen aller anderen Mitglieder und aus der Sprachbox der Gruppe gelöscht. Die persönlichen Sprachnachrichten aller Mitglieder bleiben davon unbeeinflusst.

Jedes Mitglied einer Sprachbox-Gruppe ist unter seiner eigenen Teilnehmerrufnummer erreichbar.

Bis zu 20 Mitglieder pro Sprachbox-Gruppe können eingerichtet werden.

Jeder Sprachbox-Gruppe kann ein maximal 16 Zeichen langer Name zugewiesen werden.

Mindestens ein Teilnehmer einer Sprachbox-Gruppe benötigt eine VoiceMail-Lizenz.

Abhängigkeiten

Thema	Abhängigkeit
Rufzuschaltung	Die Nutzung des Leistungsmerkmals *Rufzuschaltung* ist nicht möglich.

Verwandte Themen

- Wie Sie eine Sprachbox-Gruppe hinzufügen
- Wie Sie eine Sprachbox-Gruppe anzeigen oder ändern
- Wie Sie eine Sprachbox-Gruppe löschen
- Wie Sie ein Mitglied zur Sprachbox-Gruppe hinzufügen oder löschen
- Wie Sie ein Mitglied einer Sprachbox-Gruppe ändern

14.4.2 Faxbox-Gruppe

Durch eine Faxbox-Gruppe (Faxgruppe) kann einer bestimmten Gruppe von Teilnehmern der Zugriff auf Faxnachrichten ermöglicht werden. Über die Rufnummer der Faxbox-Gruppe wird direkt die Faxbox der Gruppe erreicht. Nachdem eine Faxnachricht auf der Faxbox der Gruppe hinterlassen wurde, erfolgt eine Weiterleitung an die Faxboxen aller Mitglieder.

Alle Mitglieder erhalten die Faxnachricht gleichzeitig. Löscht ein Mitglied der Gruppe eine Faxnachricht, wird diese auch aus den Faxboxen aller anderen Mitglieder und aus der Faxbox der Gruppe gelöscht.

Jedes Mitglied einer Faxbox-Gruppe ist unter seiner eigenen Teilnehmerrufnummer erreichbar.

Bis zu 20 Faxbox-Gruppen können eingerichtet werden.

Jeder Faxbox-Gruppe kann ein maximal 16 Zeichen langer Name zugewiesen werden.

Mindestens ein Teilnehmer einer Faxbox-Gruppe benötigt eine Fax-Lizenz.

14.4.3 Konfiguration von Sprachbox-Gruppen und Faxbox-Gruppen

Die Konfiguration von Sprachbox-Gruppen und von Faxbox-Gruppen ist ausschließlich durch einen Administrator mit dem Profil **Expert** über den **Experten-Modus** möglich.

Beschrieben ist die Vorgehensweise für folgende Anwendungsfälle, die über den **Experten-Modus** eingerichtet werden können:

- *Wie Sie eine Sprachbox-Gruppe hinzufügen*
- *Wie Sie eine Sprachbox-Gruppe anzeigen oder ändern*
- *Wie Sie eine Sprachbox-Gruppe löschen*
- *Wie Sie ein Mitglied zur Sprachbox-Gruppe hinzufügen oder löschen*
- *Wie Sie ein Mitglied einer Sprachbox-Gruppe ändern*
- *Wie Sie eine Faxbox-Gruppe konfigurieren*
- *Wie Sie eine Faxbox-Gruppe anzeigen oder ändern*
- *Wie Sie eine Faxbox-Gruppe löschen*

- *Wie Sie ein Mitglied zur Faxbox-Gruppe hinzufügen oder löschen*

14.4.3.1 Wie Sie eine Sprachbox-Gruppe hinzufügen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Kommende Rufe**.
3) Klicken Sie im Menübaum auf **Kommende Rufe > Gruppen-/Sammelanschluss**.
4) Klicken Sie auf die Registerkarte **Gruppe hinzufügen**.
5) Geben Sie im Feld **Rufnummer** die Rufnummer der neuen Sprachbox-Gruppe ein.
6) Geben Sie im Feld **Durchwahlnummer** die Durchwahlnummer der neuen Sprachbox-Gruppe ein.
7) Geben Sie im Feld **Name** den Namen der neuen Sprachbox-Gruppe ein.
8) Wählen Sie in der Aufklappliste **Typ** den Eintrag **Anrufbeantworter** aus.
9) Wählen Sie in der Aufklappliste **Rufnummer** die Rufnummer des Teilnehmers aus, der der neuen Sprachbox-Gruppe zugeordnet werden soll.
10) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Verwandte Themen

- Sprachbox-Gruppe

14.4.3.2 Wie Sie eine Sprachbox-Gruppe anzeigen oder ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Kommende Rufe**.
3) Navigieren Sie im Menübaum unter **Kommende Rufe > Gruppen-/Sammelanschluss > …** zur gewünschten Sprachbox-Gruppe.
4) Klicken Sie auf die Registerkarte **Gruppen-Parameter ändern**. Ihnen werden die aktuellen Einstellungen der Gruppen-Parameter angezeigt.

5) Ändern Sie bei Bedarf die gewünschten Parameter der Sprachbox-Gruppe.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Verwandte Themen

- Sprachbox-Gruppe

14.4.3.3 Wie Sie eine Sprachbox-Gruppe löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Kommende Rufe**.

3) Navigieren Sie im Menübaum unter **Kommende Rufe > Gruppen-/Sammelanschluss > …** zur gewünschten Sprachbox-Gruppe.

4) Klicken Sie auf die Registerkarte **Gruppe löschen**.

5) Klicken Sie auf **Löschen** und anschließend auf **OK**.

Verwandte Themen

- Sprachbox-Gruppe

14.4.3.4 Wie Sie ein Mitglied zur Sprachbox-Gruppe hinzufügen oder löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Kommende Rufe**.

3) Wählen Sie eine der folgenden Möglichkeiten:

   - Wenn Sie ein Mitglied zur Sprachbox-Gruppe hinzufügen möchten, navigieren Sie im Menübaum unter **Kommende Rufe > Gruppen-/Sammelanschluss > …** zur gewünschten Sprachbox-Gruppe. Klicken Sie auf die Registerkarte **Mitglied hinzufügen**. Wählen Sie in der Aufklappliste **Rufnummer** die Rufnummer des gewünschten Teilnehmers aus. Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

- Wenn Sie ein Mitglied aus der Sprachbox-Gruppe entfernen möchten, navigieren Sie im Menübaum unter **Kommende Rufe > Gruppen-/ Sammelanschluss > …** zum gewünschten Mitglied der Sprachbox-Gruppe ((Gruppenmitglied) Rufnummer Name). Klicken Sie auf die Registerkarte **Mitglied löschen**. Klicken Sie auf **Löschen** und anschließend auf **OK**.

Verwandte Themen

- Sprachbox-Gruppe

14.4.3.5 Wie Sie ein Mitglied einer Sprachbox-Gruppe ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Kommende Rufe**.

3) Navigieren Sie im Menübaum unter **Kommende Rufe > Gruppen-/Sammel-anschluss > …** zum gewünschten Mitglied der Sprachbox-Gruppe ((Gruppenmitglied) Rufnummer Name).

4) Klicken Sie auf die Registerkarte **Mitglied ändern**.

5) Ändern Sie die gewünschten Parameter.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Verwandte Themen

- Sprachbox-Gruppe

14.4.3.6 Wie Sie eine Faxbox-Gruppe konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Teilnehmer**.

3) Klicken Sie im Menübaum auf **Teilnehmer > Applikation-Suite > Fax Gruppe**. Angezeigt werden die bereits konfigurierten Faxbox-Gruppen.

4) Wählen Sie die nächste freie Reihe aus und geben Sie im Feld **Rufnummer** die Rufnummer der neuen Faxbox-Gruppe ein.

5) Geben Sie im Feld **DuWa** die Durchwahlnummer der neuen Faxbox-Gruppe ein.

6) Geben Sie im Feld **Name** den Namen der neuen Faxbox-Gruppe ein.

7) Wählen Sie in der Aufklappliste **Typ** den Eintag **Fax Gruppe** aus.

8) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9) Schließen Sie das Fenster **Fax Gruppe**.

10) Klicken Sie im Navigationsbaum auf **Applikationen > OpenScape Business UC Suite**.

11) Klicken Sie auf **Gruppen**.

12) Klicken Sie auf die Registerkarte **Faxgruppen**.

13) Markieren Sie die neue Faxbox-Gruppe und klicken Sie auf **Bearbeiten**.

14) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie ein Mitglied zur Faxbox-Gruppe hinzufügen möchten, markieren Sie das gewünschte Mitglied in der Liste **Benutzer**.
- Wenn Sie mehrere Mitglieder zur Faxbox-Gruppe hinzufügen möchten, drücken Sie <Strg> und markieren Sie die gewünschten Mitglieder in der Liste **Benutzer**.

15) Klicken Sie auf **Speichern**.

14.4.3.7 Wie Sie eine Faxbox-Gruppe anzeigen oder ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Teilnehmer**.

3) Klicken Sie im Menübaum auf **Teilnehmer > Applikation-Suite > Fax Gruppe**.

4) Klicken Sie im Menübaum auf die gewünschte Faxbox-Gruppe.

5) Klicken Sie auf die Registerkarte **Teilnehmer-Parameter ändern**.

6) Ändern Sie bei Bedarf die gewünschten Parameter der Faxbox-Gruppe.

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

14.4.3.8 Wie Sie eine Faxbox-Gruppe löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen > OpenScape Business UC Suite**.
3) Klicken Sie auf **Gruppen**.
4) Klicken Sie auf die Registerkarte **Faxgruppen**.
5) Markieren Sie die gewünschte Faxbox-Gruppe und klicken Sie auf **Entfernen**.

14.4.3.9 Wie Sie ein Mitglied zur Faxbox-Gruppe hinzufügen oder löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen > OpenScape Business UC Suite**.
3) Klicken Sie auf **Gruppen**.
4) Klicken Sie auf die Registerkarte **Faxgruppen**.
5) Markieren Sie die gewünschte Faxbox-Gruppe und klicken Sie auf **Bearbeiten**. Angezeigt wird die Liste **Benutzer**, in der die bereits vorhandenen Mitglieder markiert sind.
6) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie ein Mitglied zur Faxbox-Gruppe hinzufügen möchten, drücken Sie <Strg> und markieren Sie das neue Mitglied, zusätzlich zu den bereits vorhandenen Mitgliedern, in der Liste **Benutzer**.
   - Wenn Sie ein Mitglied aus der Faxbox-Gruppe entfernen möchten, drücken Sie <Strg> und entfernen Sie die Markierung des gewünschten Mitglieds in der Liste **Benutzer**.
7) Klicken Sie auf **Speichern**.

14.5 Direktansprechen für Gruppen

Direktansprechen für Gruppen ermöglicht Durchsagen an die internen Teilnehmer einer Gruppe.

14.5.1 Durchsage an Gruppe

Durchsage an Gruppe ermöglicht das Direktansprechen von internen Teilnehmern einer Gruppe. Dieses Leistungsmerkmal wird auch als "Paging Intern" bezeichnet. Gruppenmitglieder, die besetzt sind oder den Anrufschutz aktiviert haben, empfangen Paging Intern nicht. Für die gerufenen Gruppenmitglieder besteht keine Möglichkeit einer Direktantwort. Das Antworten ist nur durch Abheben des Hörers möglich, wodurch der Übergang zu einem normalen Zweiergespräch erfolgt.

Durchsage an Gruppe kann mittels einer dafür programmierten Funktionstaste oder über den Menüeintrag **Direktansprechen** oder die zugehörige Kennzahl und anschließender Wahl der Rufnummer der Zielgruppe genutzt werden. Eine Funktionstaste kann auch inklusive einer Gruppenrufnummer programmiert werden. Nach Betätigung einer solchen Funktionstaste erfolgt der sofortige Verbindungsaufbau zur programmierten Gruppe.

Abhängigkeiten

Thema	Abhängigkeit
Anrufschutz	Gruppenmitglieder mit aktiviertem Anrufschutz erhalten keine Durchsage.
ISDN-Telefone, SIP-Telefone	Das Leistungsmerkmal "Durchsage an Gruppe (Paging Intern)" kann nicht mit ISDN- oder SIP-Telefonen genutzt werden.

14.5.2 Übergabe an Gruppe aus Durchsage

Ein in Rückfrage befindliches Gespräch kann durch Übergabe aus Durchsage an eine Gruppe übergeben werden. Dazu wird eine Durchsage an die Gruppe gestartet (Paging Intern). Sobald ein Teilnehmer der Gruppe den Hörer abhebt oder den Lautsprecher aktiviert und der übergebende Teilnehmer auflegt, besteht eine Zweierverbindung. Für die anderen Gruppenmitglieder wird die Verbindung getrennt.

Durchsage an Gruppe kann mittels einer dafür programmierten Funktionstaste oder über den Menüeintrag **Direktansprechen** oder die zugehörige Kennzahl und anschließender Wahl der Rufnummer der Zielgruppe genutzt werden. Eine Funktionstaste kann auch inklusive einer Gruppenrufnummer programmiert

werden. Nach Betätigung einer solchen Funktionstaste erfolgt der sofortige Verbindungsaufbau zur programmierten Gruppe.

Abhängigkeiten

Thema	Abhängigkeit
Anrufschutz	Gruppenmitglieder mit aktiviertem Anrufschutz erhalten keine Durchsage.
ISDN-Telefone, SIP-Telefone	Das Leistungsmerkmal "Übergabe an Gruppe aus Durchsage" kann nicht mit ISDN- oder SIP-Telefonen genutzt werden.

14.6 Anrufverteilung (UCD Uniform Call Distribution)

Durch das Leistungsmerkmal "Uniform Call Distribution UCD" ermöglicht das Kommunikationssystem eine gleichmäßige Verteilung von eingehenden Anrufen auf eine Gruppe von Teilnehmern (UCD-Gruppe).

UCD-Gruppen werden vor allem im Umfeld von technischen Hotlines (zum Beispiel Kundendienst-Hotline), beim Beschwerde-Management, in der Marktforschung, Auftrags- und Bestellannahme (z. B. Versandhäuser, Ticket Service) oder auch für Notfall-Services eingesetzt.

Im Regelfall erfolgt die Anrufverteilung so, dass ein kommender Anruf an eine UCD-Gruppe an denjenigen Teilnehmer in der Gruppe (Agent) weitergeleitet wird, dessen letztes Gespräch am längsten zurückliegt. Es ist ebenfalls möglich andere Verteilungsregeln festzulegen.

Ist kein Agent frei, um einen kommenden Anruf entgegenzunehmen, wird der Anruf automatisch an eine Warteschlange (Queue) weitergeleitet. In Abhängigkeit von Priorität und Wartezeit werden die wartenden Anrufe an die frei werdenden Agenten verteilt.

Anrufern, die sich im Wartezustand befinden, können Ansagen oder Musik eingespielt werden.

Konfiguration

Mit dem Wizard **Anrufverteilung** können Sie die Gruppen und Teilnehmer für eine intelligente Anrufverteilung (UCD) konfigurieren. Beschrieben ist die Vorgehensweise für folgende Anwendungsfälle, die über den Wizard eingerichtet werden können:

- *Wie Sie eine Anrufverteilung / UCD-Gruppen konfigurieren*
- *Wie Sie UCD-Agenten hinzufügen oder löschen*
- *Wie Sie Ansagen / Wartemusik bei UCD ändern*

Neben den Konfigurationsmöglichkeiten über Wizards stehen einem Administrator mit dem Profil **Expert** zusätzliche Möglichkeiten zur Konfiguration über den **Experten-Modus** zur Verfügung.

14.6.1 Anrufverteilung / UCD-Gruppe

Eine UCD-Gruppe enthält Agenten (Teilnehmer), die zu einer Arbeitsgruppe gehören und unter einer Rufnummer zu erreichen sind. Ein ankommender interner oder externer Anruf wird automatisch dem Agenten zugeteilt, der sich am längsten in Ruhe befindet.

Jede UCD-Gruppe kann über das WBM (**Experten-Modus**) so konfiguriert werden, dass Anrufe bei einem Agenten automatisch vom Kommunikationssystem angenommen werden (Automatic Incoming Call Connection AICC).

Sind alle Agenten einer UCD-Gruppe belegt, können kommende Anrufe in eine Warteschlange eingetragen werden. Für jede UCD-Gruppe kann die maximale Anzahl der Anrufe in der Warteschlange individuell festlegt werden. Wird die maximale Anzahl der wartenden Anrufe überschritten, können die weiteren Anrufe an ein Überlaufziel (ein externes Ziel, eine andere UCD-Gruppe, ein interner Teilnehmer oder eine Gruppe) geleitet werden.

Ist das Überlaufziel eine andere UCD-Gruppe und sind auch alle Agenten dieser UCD-Gruppe belegt, bleibt der Anruf in der Warteschlange der ursprünglichen Gruppe und wird darüber hinaus in die Warteschlange der anderen UCD-Gruppe (Überlaufziel) eingereiht.

Wartenden Anrufern können Ansagen oder Musik eingespielt werden.

Jeder UCD-Gruppe kann ein maximal 16 Zeichen langer Name zugewiesen werden.

Abhängigkeiten

Thema	Abhängigkeit
Anrufumleitung	In folgenden Fällen wird der Anrufumleitung zu einer UCD-Gruppe nicht gefolgt: • Wird ein Sammelanschluss gerufen und ein Teilnehmer mit einer Anrufumleitung zu einer UCD-Gruppe ist an der Reihe, wird nicht der Anrufumleitung gefolgt. In diesem Fall wird direkt der nächste Teilnehmer des Sammelanschlusses gerufen. • Ein Teilnehmer ist Mitglied eines Gruppenrufs mit der Eigenschaft “Gruppe” und hat eine Anrufumleitung zu einer UCD-Gruppe aktiviert. • Ein Teilnehmer ist Mitglied eines Gruppenrufs im Freifall. Wird die Gruppe gerufen, wird nicht der Anrufumleitung zur UCD-Gruppe gefolgt. Ausnahme: Der erste eingetragene Teilnehmer hat eine Anrufumleitung zu einer UCD-Gruppe aktiviert. Dieser Anrufumleitung wird gefolgt.

14.6.1.1 Wie Sie eine Anrufverteilung / UCD-Gruppen konfigurieren

Mit dem Wizard **Anrufverteilung** können Sie eine intelligente Anrufverteilung auf eine Gruppe mit ausgewählten Teilnehmern konfigurieren.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > User-Telefonie**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Anrufverteilung** zu starten. Es wird Ihnen die Liste aller möglichen UCD-Gruppen angezeigt.

4) Um eine UCD-Gruppe zu konfigurieren, klicken Sie in der Zeile der gewünschten UCD-Gruppe auf **Bearbeiten**.

5) Geben Sie im Feld **Rufnummer** die Rufnummer der UCD-Gruppe ein.

6) Geben Sie im Feld **Durchwahlnummer** die Durchwahlnummer der UCD-Gruppe ein.

7) Geben Sie im Feld **Name** den Namen der UCD-Gruppe ein.

8) Klicken Sie auf **OK & Weiter**. Das Fenster **Zuweisung der UCD-Agenten** wird angezeigt.

9) Markieren Sie die gewünschten UCD-Agenten-IDs in der **Auswahl** und weisen Sie diese der UCD-Gruppe durch Klicken auf **Hinzufügen** zu.

10) Klicken Sie auf **OK & Weiter**. Das Fenster **Ansagen / Überlauf bearbeiten** wird angezeigt.

11) Wählen Sie in der Aufklappliste **Ansageeinrichtungen** die Ansageeinrichtung der UCD-Gruppe aus. Sie haben die Möglichkeit, eine Ansage (falls eingerichtet) oder die interne Wartemusik (Music On Hold MOH) auszuwählen. Nach Auswahl der Ansageeinrichtung erscheint das Feld **Ansageverzögerung**.

12) Geben Sie im Feld **Ansageverzögerung** die Zeit in Sekunden ein, nach der ein Anrufer in der Warteschlange eine Ansage erhalten soll.

13) Wählen Sie in der Aufklappliste **Zeit bis zum Ruf des nächsten Agenten** die Zeit aus, nach der ein Anruf an den nächsten UCD-Agenten der UCD-Gruppe weitergegeben werden soll.

14) Wählen Sie in der Aufklappliste **Überlauf-Ziel** das Überlauf-Ziel der UCD-Gruppe aus. Sie haben die Möglichkeit ein externes Ziel, eine andere UCD-Gruppe, einen internen Teilnehmer oder eine Gruppe auszuwählen.

Wenn Sie **Externes Ziel** als Überlauf-Ziel auswählen, erscheint das Feld **Externes Ziel** und die Aufklappliste **Richtung**.

a) Geben Sie in das Feld **Externes Ziel** die Rufnummer des externen Überlauf-Ziels ein.

b) Wenn das externe Überlaufziel über eine bestimmte Richtung erreicht werden soll, wählen Sie die gewünschte Richtung in der Aufklappliste **Richtung** aus.

15) Klicken Sie auf **OK**, um die Eingaben zu übernehmen.

16) Wenn Sie weitere UCD-Gruppen konfigurieren möchten, wiederholen Sie die Schritte 4 bis 15.

17) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

14.6.2 UCD-Agenten

Die Teilnehmer einer UCD-Gruppe (Agenten) bilden eine Arbeitsgruppe, die zum Beispiel bei technischen Hotlines oder in der Auftrags- und Bestellannahme zum Einsatz kommen kann. Alle kommenden Anrufe werden gleichmäßig auf die verfügbaren Teilnehmer einer UCD-Gruppe verteilt.

Die Zuordnung der Agenten zu den UCD-Gruppen erfolgt über Kennungen (IDs). Eine ID kann maximal einer UCD-Gruppe zugeordnet werden. Einem Agenten können mehrere IDs zugewiesen werden. Dadurch wird einem Agenten ermöglicht, in mehr als einer UCD-Gruppe zu arbeiten. Ein Agent kann jedoch nur in jeweils einer UCD-Gruppe angemeldet und damit aktiv sein.

Um die UCD-Funktionen effektiv nutzen zu können, sollten Agenten über Telefone mit Display, Funktionstasten und Headset verfügen.

Anmelden / Abmelden

Ein Agent kann sich mittels seiner ID (Kennung) an jedem Telefon (außer ISDN- und SIP-Telefonen) des Kommunikationssystems anmelden. Nach erfolgreicher Anmeldung ist der Agent verfügbar und bis zu seiner Abmeldung permanent dem betreffenden Telefon zugeordnet. Eine weitere Anmeldung an einem anderen Telefon ist nicht möglich. Nach seiner Abmeldung wird der Agent von der Anrufverteilung nicht mehr berücksichtigt.

Die UCD-Funktionen Anmelden, Abmelden und Änderung des Teilnehmerzustands können die Agenten am Telefon über dafür programmierte Funktionstasten oder über die zugehörigen Menüeinträge oder über Kennzahlen aufrufen.

Teilnehmerzustände

Nach erfolgreicher Anmeldung befindet sich ein Agent im Teilnehmerzustand **verfügbar**. Bei Bedarf kann ein Agent selbst einen anderen Teilnehmerzustand einstellen oder der Teilnehmerzustand ändert sich automatisch, in Abhängigkeit von der Agententätigkeit. Der jeweils aktuelle Teilnehmerzustand wird im Display des Telefons angezeigt.

Folgende Anzeigen sind möglich:

Anzeige	Bedeutung
verfügbar	Der Agent ist verfügbar und kann UCD-Anrufe annehmen.
nicht verfügbar	Der Agent hat sich kurzfristig von seinem Arbeitsplatz abgemeldet (zum Beispiel für eine Pause).
nachbearbeiten	Der Agent befindet sich in der Nachbearbeitungszeit. Innerhalb der Nachbearbeitungszeit erhält er keine UCD-Anrufe. Je nach Konfiguration kann es sich dabei um eine individuelle Nachbearbeitungszeit (Der Agent selbst bestimmt die Länge der Nachbearbeitungszeit durch Änderung seines Teilnehmerzustands.) oder um eine automatische Nachbearbeitungszeit (Allen Agenten steht nach einem UCD-Anruf automatisch eine Nachbearbeitungszeit zur Verfügung.) handeln.
für <UCD-Gruppenname>	Der Agent erhält einen UCD-Anruf.

Nach Ende der Arbeitszeit meldet sich ein Agent ab und steht damit für UCD-Anrufe nicht mehr zur Verfügung. Er kann weiterhin über seine persönliche Teilnehmerrufnummer erreicht werden.

Befinden sich alle Agenten einer UCD-Gruppe im Teilnehmerzustand **nicht verfügbar**, erfolgt eine Rufweiterschaltung der kommenden Anrufe an ein Überlaufziel (ein externes Ziel, eine andere UCD-Gruppe, ein interner Teilnehmer oder eine Gruppe).

Nimmt ein Agent einen Anruf nicht an, obwohl er angemeldet und verfügbar ist, wird er vom Kommunikationssystem automatisch in den Teilnehmerzustand **nicht verfügbar** versetzt.

Abhängigkeiten

Thema	Abhängigkeit
Anrufumleitung	Aktiviert ein Agent das Leistungsmerkmal "Anrufumleitung", wird er automatisch abgemeldet und steht damit für UCD-Anrufe nicht mehr zur Verfügung.
ISDN-Telefone, SIP-Telefone	Die Nutzung von ISDN- und SIP-Telefonen ist nicht möglich.

14.6.2.1 Wie Sie UCD-Agenten hinzufügen oder löschen

Mit dem Wizard **Anrufverteilung** können Sie UCD-Agenten zu einer UCD-Gruppe hinzufügen oder aus einer UCD-Gruppe löschen.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > User-Telefonie**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Anrufverteilung** zu starten. Es wird Ihnen die Liste aller möglichen UCD-Gruppen angezeigt.

4) Für das Hinzufügen oder Löschen von UCD-Agenten einer UCD-Gruppe, klicken Sie in der Zeile der gewünschten UCD-Gruppe auf **Bearbeiten**.

5) Klicken Sie auf **OK & Weiter**, um zum Fenster **Zuweisung der UCD-Agenten** zu gelangen.

6) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie UCD-Agenten hinzufügen möchten, markieren Sie die gewünschten UCD-Agenten-IDs in der **Auswahl** und weisen Sie diese der UCD-Gruppe durch Klicken auf **Hinzufügen** zu.
- Wenn Sie UCD-Agenten löschen möchten, markieren Sie die gewünschten **Mitglieder** und löschen Sie diese aus der UCD-Gruppe durch Klicken auf **Löschen**.

7) Klicken Sie auf **OK & Weiter**, um die Eingaben zu bestätigen.

8) Klicken Sie auf **OK**.

9) Wenn Sie die UCD-Agenten einer weiteren UCD-Gruppe ändern möchten, wiederholen Sie die Schritte 4 bis 8.

10) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

14.6.3 Nachbearbeitung

Durch dieses Leistungsmerkmal wird ein Agent kurzzeitig von der Anrufverteilung ausgenommen, um Nacharbeiten für den soeben beendeten Anruf durchführen zu können. Innerhalb der Nachbearbeitungszeit erhält der Agent keine UCD-Anrufe.

Es wird unterschieden zwischen

- der individuellen Nachbearbeitungszeit
  Der Agent selbst bestimmt die Länge der Nachbearbeitungszeit durch Änderung seines Teilnehmerzustands.
- der automatischen Nachbearbeitungszeit
  Dafür wird das Leistungsmerkmal "Anrufverteilung (Uniform Call Distribution UCD)" so konfiguriert, dass allen Agenten aller UCD-Gruppen nach einem UCD-Anruf automatisch eine Nachbearbeitungszeit zur Verfügung steht. Die Definition der automatischen Nachbearbeitungszeit erfolgt in Rufzyklen, das heißt in 5-Sekunden-Schritten.
  Ein Agent kann die automatische Nachbearbeitungszeit manuell verlängern, indem er seinen Teilnehmerzustand ändert.

Innerhalb der Nachbearbeitungszeit kann ein Agent weiterhin über seine persönliche Teilnehmerrufnummer erreicht werden.

14.6.3.1 Wie Sie die automatische Nachbearbeitungszeit ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Kommende Rufe**.

3) Klicken Sie im Menübaum auf **Kommende Rufe > UCD**.

4) Klicken Sie auf die Registerkarte **UCD-Parameter ändern**.

5) Wählen Sie in der Aufklappliste **Nachbearbeitungszeit (Zyklen)** die Zeit aus, die allen UCD-Agenten zur Nachbearbeitung zur Verfügung stehen soll. Die Angabe erfolgt in Rufzyklen, das heißt in 5-Sekunden-Schritten.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

14.6.4 Priorisierte Anrufordnung

Kommende interne und externe Anrufe für eine UCD-Gruppe können mit einer Priorität versehen werden. Die in der Warteschlange wartenden Anrufe werden in Abhängigkeit von der Priorität und der Wartezeit den Agenten einer UCD-Gruppe zugeteilt.

Ein wartender Anruf mit hoher Priorität wird früher beantwortet, als ein länger wartender Anruf mit niedrigerer Priorität. Ein wartender Anruf mit niedriger Priorität wird früher an ein Überlaufziel geleitet, als ein wartender Anruf mit höherer Priorität.

Für externe Anrufe erfolgt die Prioritätsvergabe leitungsbezogen (pro B-Kanal), unabhängig davon, ob es sich um IP- oder TDM-Leitungen handelt.

Beispiele:

- Kommunikationssystem mit ISDN-Primärmultiplexanschluss (S_{2M}-Schnittstelle) und ISDN-Mehrgeräteanschluss (S_0-Schnittstelle)

  Bei den über den ISDN-Primärmultiplexanschluss eingehenden Anrufen handelt es sich um normale Kundenanrufe. Alle B-Kanäle der S_{2M}-Schnittstelle erhalten dementsprechend eine mittlere Priorität. Bei Anrufen über den ISDN-Mehrgeräteanschluss handelt es sich um dringende Anrufe, wie zum Beispiel eilige Ersatzteilbestellungen. Alle B-Kanäle der S_0-Schnittstelle erhalten dementsprechend eine hohe Priorität.
- Kommunikationssystem mit Anlagenanschluss zu einem Internet-Telefonie Service Provider ITSP und einem ISDN-Mehrgeräteanschluss (S_0-Schnittstelle)

  Bei den eingehenden Anrufen über die Anlagenrufnummer für die IP-Telefonie handelt es sich um normale Kundenanrufe. Alle B-Kanäle der LAN-Schnittstelle erhalten dementsprechend eine mittlere Priorität. Bei Anrufen

über den ISDN-Mehrgeräteanschluss handelt es sich um dringende Anrufe, wie zum Beispiel eilige Ersatzteilbestellungen. Alle B-Kanäle der S_0-Schnittstelle erhalten dementsprechend eine hohe Priorität.

Für interne Anrufe wird die Priorität systemweit eingestellt und gilt damit gleichermaßen für alle internen Anrufe.

10 Prioritätsebenen (1 = hoch, 10 = niedrig) sind verfügbar.

Im Standard ist für interne Anrufe die Priorität = 10 und für externe Anrufe die Priorität = 1 eingestellt.

14.6.4.1 Wie Sie die Priorisierung der Anrufordnung ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Kommende Rufe**.

3) Klicken Sie im Menübaum auf **Kommende Rufe > UCD**.

4) Klicken Sie auf die Registerkarte **UCD-Parameter ändern**.

5) Wählen Sie in der Aufklappliste **Priorität intern** die Priorität aus, die für alle internen Anrufe an alle UCD-Gruppen gelten soll (1 = höchste Priorität, 10 = niedrigste Priorität).

6) Wählen Sie für jede Leitung (B-Kanal) in der zugehörigen Aufklappliste **Priorität** die Priorität aus, die für die externen Anrufe über diese Leitung an alle UCD-Gruppen gelten soll (1 = höchste Priorität, 10 = niedrigste Priorität). Für jeden B-Kanal kann eine individuelle Priorität eingestellt werden.

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

14.6.5 UCD-Anrufe automatisch annehmen

Durch dieses Leistungsmerkmal können Agenten kommende Anrufe ohne zusätzliche Bedienschritte annehmen (Automatic Incoming Call Connection AICC).

Um das Leistungsmerkmal nutzen zu können, muss das Telefon eines Agenten mit Headset und Trenntaste ausgestattet sein. Der Agent wird durch einen Hörton im Headset auf das Eintreffen eines Anrufes aufmerksam gemacht, der anschließend automatisch durchgeschaltet wird.

Ein bestehendes Gespräch kann ein Agent durch Drücken der Trenntaste beenden.

Standardmäßig ist das Leistungsmerkmal "AICC" nicht aktiviert. Eine Aktivierung erfolgt gruppenindividuell und gilt für alle Agenten einer UCD-Gruppe,

unabhängig davon, ob das Telefon eines Agenten mit Headset ausgestattet ist oder nicht.

14.6.5.1 Wie Sie das automatische Annehmen von UCD-Anrufen ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Kommende Rufe**.

3) Navigieren Sie im Menübaum unter **Kommende Rufe > UCD > ...** zur gewünschten UCD-Gruppe.

4) Klicken Sie auf die Registerkarte **UCD-Gruppe ändern**.

5) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn die UCD-Agenten dieser UCD-Gruppe kommende Anrufe ohne zusätzliche Bedienschritte annehmen sollen, wählen Sie in der Aufklappliste **AICC** den Eintrag **ja** aus.
- Wenn die UCD-Agenten dieser UCD-Gruppe kommende Anrufe nicht ohne die herkömmlichen Bedienschritte (zum Beispiel durch das Abnehmen des Hörers) annehmen sollen, wählen Sie in der Aufklappliste **AICC** den Eintrag **nein** aus.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

14.6.6 UCD-Warteschlange

Sind alle Agenten einer UCD-Gruppe belegt, können kommende Anrufe in eine Warteschlange eingetragen werden. Den wartenden Anrufern können Ansagen oder Musik eingespielt werden.

Wird ein Anruf in der Warteschlange für eine bestimmte Zeit (primärer Rufzyklus) nicht von dem am längsten im Zustand **verfügbar** befindlichen Agenten angenommen, wird dieser Agent in den Zustand **nicht verfügbar** versetzt. Anschließend wird der Anruf an den nächsten Agenten weitergegeben. Wird der Anruf auch von diesem Agenten nicht innerhalb einer bestimmten Zeit (sekundärer Rufzyklus) angenommen, wird auch dieser Agent in den Zustand **nicht verfügbar** versetzt. Wenn alle Agenten im Zustand **nicht verfügbar** sind, kann der Anruf an ein Überlaufziel geleitet werden.

Für jede UCD-Gruppe kann individuell festlegt werden, wie hoch die maximale Anzahl der Anrufe in der Warteschlange ist. Wird die maximale Anzahl der wartenden Anrufe überschritten, können die weiteren Anrufe an ein Überlaufziel geleitet werden.

Als Überlaufziel kann ein externes Ziel, eine andere UCD-Gruppe, ein interner Teilnehmer oder eine Gruppe definiert werden. Ist das Überlaufziel eine andere UCD-Gruppe und sind auch alle Agenten dieser UCD-Gruppe belegt, bleibt der Anruf in der Warteschlange der ursprünglichen Gruppe und wird darüber hinaus in die Warteschlange der anderen UCD-Gruppe (Überlaufziel) eingereiht.

Ein Agent kann über eine dafür programmierte Funktionstaste oder über den zugehörigen Menüeintrag oder die Kennzahl die Anzahl der Anrufe abfragen, die sich in der Warteschlange seiner UCD-Gruppe befinden.

Anrufe in einer Warteschlange

Die maximale Anzahl von Anrufen in der Warteschlange beträgt 30 für die UCD-Gruppen 1 bis 59 und 72 für die UCD-Gruppe 60.

Die minimale Anzahl von Anrufen in der Warteschlange ist Null. Ist Null als Minimalanzahl konfiguriert, gibt es keine Warteschlange. Anrufe werden direkt an ein Überlaufziel weitergeleitet oder abgewiesen, wenn kein Agent verfügbar ist.

14.6.6.1 Wie Sie eine UCD-Warteschlange ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Kommende Rufe**.

3) Navigieren Sie im Menübaum unter **Kommende Rufe > UCD > ...** zur gewünschten UCD-Gruppe.

4) Klicken Sie auf die Registerkarte **UCD-Gruppe ändern**.

5) Wählen Sie in der Aufklappliste **Prim. Rufzykl.** die Anzahl der primären Rufzyklen aus. Die Angabe erfolgt in Rufzyklen, das heißt in 5-Sekunden-Schritten. Eingestellt wird die Zeit, die ein Anruf in der Warteschlange verbleibt, falls er nicht von dem am längsten im Zustand verfügbar befindlichen Agenten angenommen wird. Anschließend wird der Anruf zum nächsten verfügbaren Agenten weitergegeben.

6) Wählen Sie in der Aufklappliste **Sek. Rufzykl.** die Anzahl der sekundären Rufzyklen aus. Die Angabe erfolgt in Rufzyklen, das heißt in 5-Sekunden-Schritten. Eingestellt wird die Zeit, die ein Anruf in der Warteschlange verbleibt, falls er nicht von dem nächsten verfügbaren Agenten angenommen wird.

7) Wählen Sie aus, ob ein Ansagewechsel stattfinden soll:

- Wenn die in der Warteschlange befindlichen Anrufer eine einmalige Ansage erhalten sollen, wählen Sie in der Aufklappliste **Ansagewechsel** den Eintrag **Einmalig** aus.

- Wenn die in der Warteschlange befindlichen Anrufer zyklisch wechselnde Ansagen erhalten sollen, wählen Sie in der Aufklappliste **Ansagewechsel** den Eintrag **Zyklisch** aus.

8) Geben Sie im Feld **Ansageverzögerung** die Zeit ein, nach der ein Anrufer in der Warteschlange eine Ansage erhält. Die Angabe erfolgt in Sekunden.

9) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

14.6.7 UCD-Überlauf

UCD-Anrufe können an ein Überlaufziel geleitet werden, falls diese nicht von den Agenten einer UCD-Gruppe angenommen werden und keine Warteschlange eingerichtet wurde oder die Maximalanzahl der Anrufe in der Warteschlange erreicht wurde.

Für jede UCD-Gruppe kann die maximale Anzahl der Anrufe in der Warteschlange individuell festlegt werden. Wird diese Anzahl überschritten, können die weiteren Anrufe an ein Überlaufziel geleitet werden.

Ist keine Warteschlange erwünscht, kann Null als maximale Anzahl der Anrufe in der Warteschlange definiert werden. Nicht angenommene Anrufe werden dann sofort an ein Überlaufziel geleitet.

Abhängigkeiten

Thema	Abhängigkeit
AutoAttendant	Die Verwendung eines AutoAttendants als Überlaufziel ist nicht möglich.

14.6.7.1 Wie Sie den UCD-Überlauf ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Kommende Rufe**.

3) Navigieren Sie im Menübaum unter **Kommende Rufe > UCD > ...** zur gewünschten UCD-Gruppe.

4) Klicken Sie auf die Registerkarte **UCD-Gruppe ändern**.

5) Geben Sie im Feld **Wart. Anrufe** die maximale Anzahl der wartenden Anrufe ein. Die über diese Anzahl hinausgehenden Anrufe werden an ein Überlaufziel geleitet.

6) Geben Sie im Feld **Overflow-Zeit** die gewünschte Zeit ein. Die Angabe erfolgt in Sekunden.

Hinweis: Diese Einstellung ist ausschließlich relevant, wenn eine externe UCD-Applikation angeschlossen ist. Wird ein wartender Anruf nicht innerhalb der Overflow-Zeit durch die UCD-Applikation angenommen, wird der Anruf anhand der Angaben im Call Management durch das Kommunikationssystem weiterverarbeitet.

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

14.6.8 UCD-Nachtschaltung

Für jede UCD-Gruppe kann eine individuelle Nachtschaltung konfiguriert werden. Jeder Agent einer UCD-Gruppe kann die Nachtschaltung aktivieren und deaktivieren. Nach der Aktivierung werden alle Anrufe für diese UCD-Gruppe zum Nachtziel geleitet.

Als Nachtschaltungsziel kann zum Beispiel ein interner Teilnehmer, eine andere Gruppe, eine Ansage/Wartemusik, die Sprachbox des Kommunikationssystems oder ein externes Ziel definiert werden.

Aktivierung / Deaktivierung

Die Aktivierung oder Deaktivierung der UCD-Nachtschaltung kann mittels einer dafür programmierten Funktionstaste oder über die zugehörigen Menüeinträge oder die Kennzahlen erfolgen. Mit der Aktivierung ist die Rufnummer des gewünschten Nachtschaltungsziels einzugeben.

Informationen zur Nachtschaltung des Kommunikationssystems siehe *Nachtschaltung*.

Abhängigkeiten

Thema	Abhängigkeit
Teilnehmerzustand	Eine Aktivierung der UCD-Nachtschaltung verändert nicht den jeweils aktuellen Teilnehmerzustand der einzelnen Agenten. Die Zwangsabmeldung der noch angemeldeten Agenten erfolgt nicht.
Nachtschaltung des Kommunikationssystems	Die UCD-Nachtschaltung und die Nachtschaltung des Kommunikationssystems können unabhängig voneinander aktiviert und deaktiviert werden. Beispiel: Eine UCD-Gruppe wurde als Nachtschaltungsziel des Kommunikationssystems eingetragen. Anrufe, die diese UCD-Gruppe über die Nachtschaltung des Kommunikationssystems erreichen, verbleiben in dieser UCD-Gruppe, unabhängig von einer UCD-Nachtschaltung.
Bestehende Gespräche	Bestehende Gespräche werden durch die Aktivierung der UCD-Nachtschaltung nicht beeinflusst.

14.6.9 Ansagen / Wartemusik bei UCD

Anrufern können Wartemusik (Music On Hold MOH) oder Ansagen eingespielt werden, falls diese nicht sofort an die Agenten einer UCD-Gruppe vermittelt werden. Wartemusik und Ansagen können jeder UCD-Gruppe individuell zugeordnet werden.

Es bestehen folgende Möglichkeiten:

- Wartemusik (Music On Hold MOH)
  Wartenden Anrufern kann Musik aus der integrierten Quelle des Kommunikationssystems eingespielt werden. Zusätzliche Wartemusik-Dateien können von einem PC in das Kommunikationssystem geladen werden.
  Weitere Informationen siehe *Wartemusik*
- Ansagen
  Wartenden Anrufern können integrierte Ansagen eingespielt werden. Zusätzliche Ansagen können von einem PC in das Kommunikationssystem geladen werden.
  Weitere Informationen siehe *Ansagen*

Die Zeit bis zum Start der Ansage ist einstellbar (**Ansageverzögerung**). Um die Ansage zu unterdrücken, kann der Höchstwert (600 Sekunden) eingestellt werden. Dabei wird angenommen, dass der Anruf innerhalb dieser Zeit angenommen wird.

14.6.9.1 Wie Sie Ansagen / Wartemusik bei UCD ändern

Mit dem Wizard **Anrufverteilung** können Sie Ansagen und/oder Wartemusik für UCD-Gruppen konfigurieren.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > User-Telefonie**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Anrufverteilung** zu starten. Es wird Ihnen die Liste aller möglichen UCD-Gruppen angezeigt.

4) Um die Ansagen / Wartemusik (Music On Hold MOH) einer UCD-Gruppe zu ändern, klicken Sie in der Zeile der gewünschten UCD-Gruppe auf **Bearbeiten**.

5) Klicken Sie so oft auf **OK & Weiter**, bis das Fenster **Ansagen / Überlauf bearbeiten** angezeigt wird.

6) Wählen Sie in der Aufklappliste **Ansageeinrichtungen** die Ansageeinrichtung der UCD-Gruppe aus. Sie haben die Möglichkeit, eine Ansage (falls eingerichtet) oder die interne Wartemusik (Music On Hold MOH) auszu-

wählen. Nach Auswahl der Ansageeinrichtung erscheint das Feld **Ansageverzögerung**.

7) Geben Sie im Feld **Ansageverzögerung** die Zeit in Sekunden ein, nach der ein Anrufer in der Warteschlange eine Ansage erhalten soll.

8) Klicken Sie auf **OK**, um die Eingaben zu übernehmen.

9) Wenn Sie die Ansagen / Wartemusik (Music On Hold MOH) einer weiteren UCD-Gruppe ändern möchten, wiederholen Sie die Schritte 4 bis 8.

10) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

14.6.10 Übergabe an UCD-Gruppen

Interne und externe Gespräche können UCD-Gruppen übergeben werden. Wird ein Anruf innerhalb einer bestimmten Zeit nicht angenommen, erfolgt ein Wiederanruf.

Die Wiederanrufzeit wird über den Zeitparameter **Überwachung eines Übergeben vor Melden an eine UCD-Gruppe** definiert. Die Standardeinstellung beträgt 300 Sekunden. Eine Änderung dieser Einstellung ist durch einen Administrator mit dem Profil **Expert** über den **Experten-Modus** möglich (von 0 bis 255 Minuten).

Abhängigkeiten

Thema	Abhängigkeit
Ansagen	Den übergebenen externen Gesprächen können Ansagen eingespielt werden. Bei internen Gesprächen ist das nicht möglich.
Wiederanrufzeit	Für eine Übergabe an UCD-Gruppen gilt eine andere Wiederanrufzeit als für eine Übergabe an Teilnehmer.

14.6.10.1 Wie Sie die Wiederanrufzeit für übergebene Gespräche an UCD-Gruppen ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **Grundeinstellungen > System > Zeitparameter**.

4) Geben Sie für den Zeitparameter **Überwachung eines Übergeben vor Melden an eine UCD-Gruppe** die gewünschte Wiederanrufzeit an (einstellbar von 0 bis 255 Minuten, Standardeinstellung = 300 Sekunden). Wird ein Gespräch nach Ablauf dieser Zeit nicht angenommen, erfolgt ein Wiederanruf.

a) Wählen Sie in der Aufklappliste **Basis** die gewünschte Zeitbasis aus.

b) Geben Sie im Feld **Faktor** den Wert ein, mit dem die Zeitbasis multipliziert werden soll.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

14.6.11 Auslösen von UCD-Anrufen über analoge Leitungen

Werden UCD-Anrufe über analoge Leitungen nicht innerhalb einer bestimmten Zeit angenommen, werden diese Anrufe ausgelöst. Damit wird ein Hängenbleiben von analogen Leitungen verhindert.

Die Auslösezeit wird über den Zeitparameter **Überwachung eines UCD-Rufes auf einer analogen Leitung** definiert. Die Standardeinstellung beträgt 300 Sekunden. Eine Änderung dieser Einstellung ist durch einen Administrator mit dem Profil **Expert** über den **Experten-Modus** möglich (von 0 bis 255 Minuten).

14.6.11.1 Wie Sie die Auslösezeit für UCD-Anrufe über analoge Leitungen ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **Grundeinstellungen > System > Zeitparameter**.

4) Geben Sie für den Zeitparameter **Überwachung eines UCD-Rufes auf einer analogen Leitung** die gewünschte Auslösezeit an (einstellbar von 0 bis 255 Minuten, Standardeinstellung = 300 Sekunden). Wird ein Anruf nach Ablauf dieser Zeit nicht angenommen, wird dieser Anruf ausgelöst.

a) Wählen Sie in der Aufklappliste **Basis** die gewünschte Zeitbasis aus.

b) Geben Sie im Feld **Faktor** den Wert ein, mit dem die Zeitbasis multipliziert werden soll.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

15 Anruf-Routing

Das Kommunikationssystem bietet verschiedene Möglichkeiten Anrufe einem gewünschten Ziel zuzuordnen, wie Berechtigungen (Wahlkontrolle), Tag- und Nachtschaltung, Least Cost Routing und Anrufsteuerungsdienst. Das Absetzen von Notrufen ist aus jeder Konfiguration möglich.

15.1 Berechtigungen (Wahlkontrolle)

Berechtigungen (Wahlkontrolle) regeln den Zugang der Teilnehmer zu möglicherweise kostenpflichtigen externen Verbindungen.

15.1.1 Berechtigungsgruppen und Berechtigungsklassen

Jedem Teilnehmer ist eine Berechtigungsgruppe zugeordnet, in der definiert ist, welche Berechtigung der Teilnehmer für kommende und gehende Anrufe hat.

In der Berechtigungsgruppe ist für jede Richtung eine der folgenden Berechtigungsklassen definiert:

- **Intern**
  Der Teilnehmer darf nur intern telefonieren.
- **Halbamt**
  Der Teilnehmer darf externe Gespräche nur annehmen.
- **Erlaubnisliste** 1-6
  Der Teilnehmer darf nur die in der Erlaubnisliste definierten externen Rufnummern wählen. Ist keine Rufnummer eingetragen gilt Halbamtsberechtigung.
- **Verbotsliste** 1-6
  Der Teilnehmer darf die in der Verbotsliste definierten externen Rufnummern nicht wählen. Ist keine Rufnummer eingetragen gilt Vollamtsberechtigung.
- **Vollamt**
  Der Teilnehmer darf ohne Einschränkung kommende und gehende externe Gespräche annehmen und aufbauen.

Einige der 15 möglichen Berechtigungsgruppen sind für alle Richtungen mit der gleichen Berechtigungsklasse vorbelegt und aussagekräftig benannt (z. B. Berechtigungsgruppe **International** mit der Berechtigungsklasse **Vollamt** oder Berechtigungsgruppe **Kommend** mit der Berechtigungsklasse **Halbamt**. Die Namen aller Berechtigungsgruppen können vom Administrator geändert werden.

Abhängigkeiten

Thema	Abhängigkeit
Kurzwahlziele	Zentrale Kurzwahlziele können unabhängig von zugeordneten Berechtigungsgruppe angewählt werden.
LCR	Berechtigungsgruppen (Wahlkontrolle) und LCR-Berechtigung sind unterschiedlich.
Anrufumleitung	Bei einer Anrufumleitung gilt die Berechtigung des Anrufenden.

15.1.1.1 Wie Sie den Namen einer Berechtigungsgruppe ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Berechtigungen**.

3) Klicken Sie im Menübaum auf **Tag:Berechtigsgruppe**.

> ***INFO:*** Sie können im Menübaum auch auf **Nacht:Berechtigsgruppe** klicken, das führt zum selben Ergebnis.

4) Klicken Sie im Menübaum auf die gewünschte Berechtigungsgruppe.

5) Klicken Sie auf die Registerkarte **Berechtigungsgruppe ändern**.

6) Ändern Sie im Feld **Berechtigungsgruppe** den Namen der Berechtigungsgruppe.

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

15.1.1.2 Wie Sie die Berechtigungsklassen einer Berechtigungsgruppe ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Berechtigungen**.

3) Klicken Sie im Menübaum auf **Tag:Berechtigsgruppe**.

4) Klicken Sie im Menübaum auf die gewünschte Berechtigungsgruppe.

5) Klicken Sie auf die Registerkarte **Berechtigungsgruppe ändern**.

6) Wählen Sie für den Tag-Betrieb bei jeder genutzten Richtung aus der Aufklappliste die gewünschte Berechtigungsklasse aus.

7) Wählen Sie bei Bedarf die Berechtigungsklasse für **Networking** für den Tag-Betrieb.

8) Klicken Sie im Menübaum auf **Nacht:Berechtigungsgruppe**.

9) Klicken Sie im Menübaum auf die zuvor bearbeitete Berechtigungsgruppe.

10) Klicken Sie auf die Registerkarte **Berechtigungsgruppe ändern**.

11) Wählen Sie jetzt für den Nacht-Betrieb bei jeder genutzten Richtung aus der Aufklappliste die gewünschte Berechtigungsklasse aus.

12) Wählen Sie auch hier bei Bedarf die Berechtigung für **Networking** für den Nacht-Betrieb.

13) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

15.1.1.3 Wie Sie alle Teilnehmer einer Berechtigungsgruppe anzeigen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Berechtigungen**.

3) Klicken Sie im Menübaum auf **Tag:Berechtigsgruppe**.

> ***INFO:*** Sie können im Menübaum auch auf **Nacht:Berechtigsgruppe** klicken, das führt zum selben Ergebnis.

4) Klicken Sie im Menübaum auf die gewünschte Berechtigungsgruppe.

5) Klicken Sie auf die Registerkarte **Gruppenmitglieder anzeigen**. Alle Teilnehmer, denen die ausgewählte Berechtigungsgruppe zugewiesen ist, werden Ihnen mit Rufnummer und Name angezeigt.

15.1.2 Erlaubnis- und Verbotslisten

Mit Erlaubnis- und Verbotslisten kann festgelegt werden, welche externen Rufnummern die Teilnehmer wählen dürfen und welche nicht.

Erlaubnislisten enthalten die am Anfang einer Rufnummer zulässigen Ziffernfolgen. Der Teilnehmer darf nur die in der Erlaubnisliste definierten externen Rufnummern wählen. Stellen Sie sicher, dass in der Liste auch alle benötigten Notrufnummern enthalten sind!

Verbotslisten enthalten die am Anfang einer Rufnummer unzulässigen Ziffernfolgen. Der Teilnehmer darf die in der Verbotsliste definierten externen Rufnummern nicht wählen. Stellen Sie sicher, dass in der Liste keine Notrufnummern enthalten sind!

Die **Liste der Notrufnummern** ist ein Spezialfall der Erlaubnisliste. Der Teilnehmer darf nur die in der Liste erfassten Notrufnummern wählen. Stellen Sie sicher, dass in der Liste alle benötigten Notrufnummern enthalten sind!

In die Listen müssen nicht die vollständigen Rufnummern eingetragen werden. Um Teilnehmer beispielsweise zur Anwahl aller (kostenlosen) 0800xxxer-Nummern zu berechtigen, muss hier lediglich die `0800` eingeben werden. Da sich die Listen nur auf gehende Externgespräche beziehen, muss die Amtskennzahl bei den eingetragenen Rufnummern nicht mit angegeben werden. Der Eintrag des Zeichens `#` an erster Stelle einer verbotenen Rufnummer verhindert eine Umgehung der Wahlkontrolle für Systemtelefone, die eine analoge Amtsleitung mit MFV-Wahlverfahren belegen und während der Wahl auf MFV umschalten wollen.

Über **Auswertungsfilter** kann der Administrator zu einer beliebigen Verbotsliste festlegen, welche Ziffern nicht mit der entsprechenden Verbotsliste verglichen werden sollen. Das Kommunikationssystem blendet den eingestellten Ziffernbereich vor der Wahlbewertung aus. Durch ein Verbot der Zeichen `*` und `#` wird erreicht, dass ein Teilnehmer bei der Eingabe dieser Zeichen die Wahlkontrolle umgehen kann.

Konfigurationsgrenzen

Merkmal	Anzahl
Erlaubnisliste 1: lang, 100 Einträge	1
Erlaubnislisten 2-6: kurz, 10 Einträge	5
Verbotsliste 1: lang, 50 Einträge	1
Verbotslisten 2-6: kurz, 10 Einträge	5
Zeichenlänge der Listeneinträge (Ziffern 0 - 9 sowie die Zeichen * und #)	26

15.1.2.1 Wie Sie eine Notrufnummernliste erstellen

Mit dem Wizard **Berechtigung** können Sie eine Liste mit Notrufnummern für die Berechtigungsgruppe "Notrufnummern" erstellen.

Voraussetzungen

- Sie sind am WBM angemeldet.
- Das Kommunikationssystem ist an eine Amtsleitung angeschlossen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards > User-Telefonie**.
3) Klicken Sie auf **Bearbeiten** um den Wizard **Berechtigung** zu starten.
4) Geben Sie im Eingabefeld eine Notrufnummer ein und klicken Sie auf **Hinzufügen**. Die Rufnummer wird in die Liste der Notrufnummern übernommen.
5) Wenn Sie weitere Rufnummern in die Notrufnummernliste eintragen wollen, wiederholden Sie den vorherigen Schritt.
6) Klicken Sie so oft auf **OK & Weiter** bis Sie mit **Beenden** die Konfiguration abschließen.

15.1.2.2 Wie Sie eine Erlaubnis- und eine Verbotsliste erstellen

Mit dem Wizard **Berechtigung** können Sie eine Erlaubnisliste und eine Verbotsliste erstellen.

Voraussetzungen

- Sie sind am WBM angemeldet.
- Das Kommunikationssystem ist an eine Amtsleitung angeschlossen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards > User-Telefonie**.
3) Klicken Sie auf **Bearbeiten** um den Wizard **Berechtigung** zu starten.
4) Klicken Sie auf **OK & Weiter**.
5) Geben Sie im Eingabefeld eine erlaubte Rufnummer ohne Amtskennzahl ein und klicken Sie auf **Hinzufügen**. Die Rufnummer wird in die Erlaubnisliste übernommen.
6) Wenn Sie weitere Rufnummern in die Erlaubnisliste eintragen wollen, wiederholden Sie den vorherigen Schritt.
7) Klicken Sie auf **OK & Weiter**.
8) Geben Sie im Eingabefeld eine verbotene Rufnummer ohne Amtskennzahl ein und klicken Sie auf **Hinzufügen**. Die Rufnummer wird in die Verbotsliste übernommen.
9) Wenn Sie weitere Rufnummern in die Verbotsliste eintragen wollen, wiederholden Sie den vorherigen Schritt.
10) Klicken Sie so oft auf **OK & Weiter** bis Sie mit **Beenden** die Konfiguration abschließen.

15.1.2.3 Wie Sie weitere Erlaubnislisten erstellen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Berechtigungen**.

3) Klicken Sie im Menübaum auf **Berechtigungen > Erlaubnislisten**.

4) Klicken Sie im Menübaum auf die gewünschte Erlaubnisliste.

5) Klicken Sie auf die Registerkarte **Rufnummer hinzufügen**.

6) Geben Sie die externe **Rufnummer** ohne Richtungskennzahl ein.

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

8) Wenn Sie weitere Rufnummern hinzufügen wollen, wiederholen Sie die Schritte 6 und 7.

9) Wenn Sie weitere Erlaubnislisten erstellen wollen, wiederholen Sie die Schritte 4 bis 7.

10) In der Registerkarte **Liste anzeigen** können Sie sich alle Rufnummern der ausgewählten Erlaubnisliste anzeigen lassen.

15.1.2.4 Wie Sie weitere Verbotslisten erstellen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Berechtigungen**.

3) Klicken Sie im Menübaum auf **Berechtigungen > Verbotslisten**.

4) Klicken Sie im Menübaum auf die gewünschte Verbotsliste.

5) Klicken Sie auf die Registerkarte **Rufnummer hinzufügen**.

6) Geben Sie die externe **Rufnummer** ohne Richtungskennzahl ein.

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

8) Wenn Sie weitere Rufnummern hinzufügen wollen, wiederholen Sie die Schritte 6 und 7.

9) Wenn Sie weitere Verbotslisten erstellen wollen, wiederholen Sie die Schritte 4 bis 7.

10) In der Registerkarte **Liste anzeigen** können Sie sich alle Rufnummern der ausgewählten Verbotsliste anzeigen lassen.

15.1.2.5 Wie Sie alle Rufnummern einer Verbotsliste anzeigen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Berechtigungen**.

3) Klicken Sie im Menübaum auf **Berechtigungen > Verbotslisten**.

4) Klicken Sie im Menübaum auf die Verbotsliste mit der gewünschten Nummer.

15.1.2.6 Wie Sie alle Rufnummern einer Erlaubnisliste anzeigen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Berechtigungen**.

3) Klicken Sie im Menübaum auf **Berechtigungen > Erlaubnislisten**.

4) Klicken Sie im Menübaum auf die Erlaubnisliste mit der gewünschten Nummer.

15.1.2.7 Wie Sie den Auswertungsfilter für eine Verbotsliste ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Berechtigungen**.

3) Klicken Sie im Menübaum auf **Berechtigungen > Verbotslisten**.

4) Klicken Sie im Menübaum auf die Verbotsliste mit der gewünschten Nummer.

5) Klicken Sie auf die Registerkarte **Auswertungsfilter ändern**.

6) Wählen Sie in den Aufklapplisten **ab Ziffer** und **bis Ziffer** einen Bereich aus.

Ein Bereich innerhalb einer Rufnummer ist hiermit konfigurierbar. Die Start-Position des Bereichs wird über die Klappliste **ab Ziffer**, die Ende-Position über **bis Ziffer** ausgewählt. .

Die Vorbelegung dieses Feldes mit ***** und **#** ist zur Sperrung dieser Zeichen gedacht, denn * und # könnten als "Dummy"-Zeichen verwendet werden, die im Amt nicht ausgewertet werden und damit eine Wahlkontrolle umgehen. Durch Eingabe von * und # in die Verbotsliste haben diese Zeichen keinen Einfluß und nur die gewählten Ziffern werden ausgewertet.

7) Geben Sie im Feld **Zeichen** das oder die auszublendende(n) Zeichen ein.

8) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

15.1.3 Nachtschaltung

Während der Nacht können kommende und gehende Anrufe anders behandelt werden als während des Tages. Kommende Anrufe können zu einem Nachtschaltungsziel umgeleitet werden und interne Teilnehmer können andere Berechtigungen für ihr Telefon haben als tagsüber. Die systemweite Umschaltung zwischen Tag- und Nacht-Betrieb wird automatisch zu einem vom Administrator vorgegebenen Zeitpunkt durchgeführt.

Jedes Telefon kann als Nachtschaltungsziel dienen, sofern die zugehörige Berechtigungsgruppe ankommende Rufe gestattet. Ein Telefon mit nur interner Berechtigung kann nicht als Nachtschaltungsziel eingetragen werden. Hat das Nachtschaltungsziel eine Anrufumleitung aktiviert, so wird dieser gefolgt.

Einer Berechtigungsgruppe können im Nacht-Betrieb andere Berechtigungsklassen zugewiesen sein als im Tag-Betrieb, um z. B. Gebührenmissbrauch vorzubeugen.

Für den Nachtbetrieb können Sie zusätzlich einen anderen Abwurfplatz festlegen als für den Tag-Betrieb. Der Abwurfplatz kann ein einzelner Teilnehmer oder eine Gruppe sein.

Zeitgesteuerte Nachtschaltung

Das Kommunikationssystem aktiviert und deaktiviert die Nachtschaltung nach einem vom Administrator festgelegten Zeitplan.

> ***INFO:*** Bei der zeitgesteuerten Nachtschaltung gilt die eingestellte Regelung für ALLE Teilnehmer des Kommunikationssystems. Es gibt auch eine automatische Berechtigungsumschaltung nach Zeit, dabei werden Teilnehmer zu Gruppen (Profilen) zusammengefasst.

Variable Nachtschaltung

Die variable Nachtschaltung wird manuell von einem berechtigten Teilnehmer aktiviert und deaktiviert. Die Anrufe folgen den vom Administrator konfigurierten Rufziellisten.

Standardmäßig kann der erste Teilnehmer (die Rufnummer "100") im Kommunikationssystem die Nachtschaltung aktivieren und deaktivieren. Der Administrator kann bis zu fünf Teilnehmer dazu berechtigen, die Nachtschaltung zu aktivieren und deaktivieren.

UCD-Nachtschaltung

Für jede UCD-Gruppe können Sie eine individuelle Nachtschaltung konfigurieren. Diese ist unabhängig von der systemweiten Nachtschaltung aktivierbar und deaktivierbar. Jeder Agent einer UCD-Gruppe kann diese aktivieren und deaktivieren. Der jeweils aktuelle Status der einzelnen Agenten sowie bestehende Gespräche sind davon nicht berührt. Nach der Aktivierung werden alle Anrufe für diese UCD-Gruppe zum Nachtschaltungsziel geleitet.

Als Nachtschaltungsziel ist eine andere UCD-Gruppe, ein interner Teilnehmer oder ein externes Ziel möglich.

15.1.3.1 Wie Sie Berechtigungen für die manuelle Nachtschaltung vergeben

Mit dem Wizard **Berechtigungen** vergeben Sie die Berechtigung für einzelne Teilnehmer, die das Kommunikationssystem über Ihr Telefon von Tag- auf Nachtschaltung (und umgekehrt) umschalten können. Die Umschaltung zwischen Tag- und Nachtschaltung erfolgt über das Telefon durch eine Kennzahl.

Voraussetzungen

- Sie sind am WBM angemeldet. Das Kommunikationssystem ist an eine Amtsleitung angeschlossen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > User-Telefonie**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Berechtigung** zu starten.

4) Klicken Sie so oft auf **OK & Weiter** bis Sie das Fenster **Berechtigte Teilnehmer für Nachtschaltung** sehen.

5) Markieren Sie den gewünschten Teilnehmer in der Liste unter **Teilnehmer** und klicken Sie auf **Hinzufügen**. Der Teilnehmer erscheint anschließend in der Liste unter **Berechtigte Teilnehmer**.

6) Klicken Sie auf **OK & Weiter**.

7) Im Fenster **Systemüberblick** sehen Sie eine Aufstellung über alle vergebenen Berechtigungen.

8) Klicken Sie auf **Beenden**.

15.1.3.2 Wie Sie Berechtigungen für die manuelle Nachtschaltung löschen

Mit dem Wizard **Berechtigungen** können Sie die Berechtigung von Teilnehmern für die Umschaltung von Tag- auf Nachtschaltung löschen.

Voraussetzungen

- Sie sind am WBM angemeldet. Das Kommunikationssystem ist an eine Amtsleitung angeschlossen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > User-Telefonie**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Berechtigung** zu starten.

4) Klicken Sie so oft auf **OK & Weiter** bis Sie das Fenster **Berechtigte Teilnehmer für Nachtschaltung** sehen.

5) Markieren Sie den gewünschten Teilnehmer (dessen Berechtigung Sie löschen wollen) in der Liste unter **Berechtigte Teilnehmer** und klicken Sie auf **Löschen**.

6) Klicken Sie auf **OK & Weiter**.

7) Im Fenster **Systemüberblick** sehen Sie eine Aufstellung über alle vergebenen Berechtigungen.

8) Klicken Sie auf **Beenden**.

15.1.3.3 Wie Sie die zeitgesteuerte Nachtschaltung konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Berechtigungen**.

3) Klicken Sie im Menübaum auf **Automatische Nachtschaltung > Montag** (Montag als Beispiel; alle Tage der Woche stehen zur Auswahl).

4) Wählen Sie unter **Bearbeiten Zone** eine von vier möglichen Zonen aus, für die eine bestimmte Berechtigung gelten sollte.

5) Legen Sie mit **Beginn** und **Ende** die Zeit (in Stunden und Minuten) für diese Berechtigung fest.

6) Wählen Sie unter **Nacht Ruf-Nr**. den berechtigten Teilnehmer aus.

Im Feld **Autom. Nacht Service** wird Ihre Einstellung für die jeweilige Zone angezeigt.

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

15.1.3.4 Wie Sie einen Sondertag für die zeitgesteuerte Nachtschaltung konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Berechtigungen**.

3) Klicken Sie im Menübaum auf **Berechtigungen > Sondertage**.

4) Wählen Sie mit **>>** oder **<<** das Jahr, für das Sie einen Feiertag festlegen möchten.

5) Wählen Sie mit **>>** oder **<<** den Monat, für den Sie einen Feiertag festlegen möchten.

6) Klicken Sie im Kalender auf den Tag, den Sie als Feiertag festlegen möchten.

7) Geben Sie unter **Name** die Bezeichnung des Feiertags ein.

8) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

15.1.3.5 Wie Sie einen Sondertag für die zeitgesteuerte Nachtschaltung löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Berechtigungen**.

3) Klicken Sie im Menübaum auf **Berechtigungen > Automatische Nachtschaltung > Sondertage**.

4) Klicken Sie unter **Tag** links von dem zu löschenden Feiertag auf den Papierkorb.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

15.1.4 Automatische Berechtigungsumschaltung nach Zeit

Bei der automatischen Berechtigungsumschaltung nach Zeit werden die Teilnehmer in sogenannte Teilnehmer-Profile zusammengefasst, in denen definiert ist, welche Berechtigungsgruppe in welchem Zeitintervall der Woche gültig ist. Für jedes Teilnehmer-Profil kann ein Zeitplan konfiguriert werden.

Unterschiede zwischen der automatischen Berechtigungsumschaltung nach Zeit und der zeitgesteuerten Nachtschaltung:

- Die automatische Berechtigungsumschaltung nach Zeit gilt nur für den Tagbetrieb und nicht für die Nachtschaltung.
- Erreichen des Anrufziels über Call Management:
  Die Abwicklung erfolgt über das Call Management und ist unabhängig von der automatischen Berechtigungsumschaltung nach Zeit. Es gibt verschiedene Anruflisten für Tag und Nacht.
- Bei der zeitgesteuerten Nachtschaltung kann nur zwischen Tag- und Nachtschaltung unterschieden werden und sie gilt für ALLE Teilnehmer.
- Abwurfziele
  Das Abwurfziel wird nur durch die zeitgesteuerte Nachtschaltung bestimmt.
- Berechtigungsgruppe:
  Während der Nacht ist die Berechtigungsgruppe in einer konstanten (konfigurierbaren) Relation zum Teilnehmer, die automatische Berechtigungsumschaltung nach Zeit hat darauf keinen Einfluss.
  Während des Tages kann die Berechtigungsgruppe zwischen bestimmten Tageszeiten wechseln oder ist ebenfalls in einer festen (konfigurierbaren) Relation zum Teilnehmer.

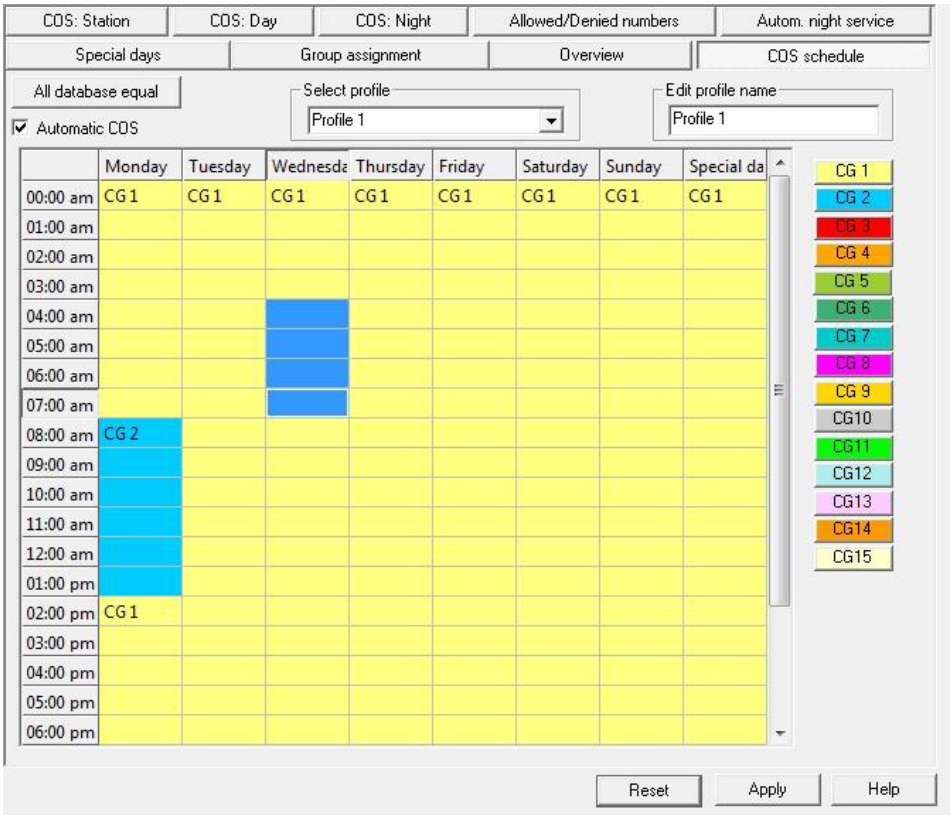
Abhängigkeiten

Thema	Abhängigkeiten
Nachtschaltung	Das Leistungsmerkmal “ Nachtschaltung" hat Priorität vor dem Leistungsmerkmal “Automatische Berechtigungsumschaltung nach Zeit". Wenn die Nachtschaltung aktiviert ist , wird die Berechtigungsgruppe wie gewohnt gehandhabt und die Berechtigungsgruppe für die Nacht übernommen. Der Zeitplan ist nur tagsüber relevant.
Vernetzung	Die automatische Berechtigungsumschaltung und die Nachtumschaltung funktionieren nicht knotenübergreifend.

15.1.4.1 Zeitplan

Der Zeitplan dient der Steuerung der Berechtigungsklassen bei der automatischen Berechtigungsumschaltung nach Zeit. Es ist möglich bis zu acht Berechtigungsumschaltungen pro Tag für jeden Tag der Woche zu konfigurieren.

Jeder Tag beginnt um 00:00 Uhr. Die Eingabe der Ende-Zeit in den einzelnen Spalten markiert die Zeitzonen. Im folgenden Beispiel für einen Zeitplan sind die einzelnen Berechtigungsumschaltungen mit CG2, CG4 und CG5 bezeichnet.



Ein Teilnehmer kann unterschiedliche Berechtigungsgruppen für Tag und Nacht haben.

Wenn systemweit die automatische Berechtigungsumschaltung für den Tag gesetzt ist, hat ein Teilnehmer die ihm zugewiesene Berechtigungsgruppe je nach eingestelltem Profil und Zeitplan. In der Nacht hat der Teilnehmer die gleiche Berechtigungsgruppe die ihm bisher (über die Nachtschaltung) zugewiesen wurde.

Die automatische Berechtigungsumschaltung nach Zeit ist standardmäßig deaktiviert

Das Kommunikationssystem unterstützt nur eine Zeitzone (Weltzeit). Abgesetzte Teilnehmergruppen, die in unterschiedlichen Zeitzonen arbeiten, werden auf die Zeitzone des Kommunikationssystems gesetzt.

Der Zeitplan kann nur über den Manager E konfiguriert werden.

15.1.5 VBZ (Verkehrsbeziehungen)

Über das Leistungsmerkmal VBZ (Verkehrsbeziehungen) wird festgelegt, welche Teilnehmer des Kommunikationssystems Verbindungen zu welchen anderen Teilnehmern herstellen können. Dieses Leistungsmerkmal wird z. B. für Teilanlagen verwendet.

Durch VBZ lässt sich ebenfalls einrichten, auf welche Leitungen die einzelnen Teilnehmer für kommende und gehende Rufe Zugriff haben.

Die VBZ-Funktionalität greift nicht auf die Applikationen zu, sie hat ausschließlich für die Telefonie Bedeutung. Die Darstellung des Anwesenheitsstatus z. B. wird nicht über eine Zugriffsbeschränkung durch VBZ verhindert.

Das Leistungsmerkmal VBZ wird in zwei Schritten realisiert:

- VBZ-Gruppen bilden
- VBZ-Matrix konfigurieren

INFO: Das Leistungsmerkmal VBZ sollte nicht in Verbindung mit UC-Funktionalität genutzt werden, da es Einschränkungen zur Folge hätte.

15.1.5.1 VBZ-Gruppen (Verkehrsbeziehungsgruppen)

VBZ-Gruppen (Verkehrsbeziehungsgruppen) regeln erlaubte und verbotene Verbindungen zwischen Teilnehmern und Leitungen des Kommunikationssystems.

Mit Hilfe von VBZ-Gruppen können bestimmte Teilnehmer und Leitungen zu Gruppen zusammen geschlossen werden.

Über VBZ-Gruppenzuordnung weisen Sie den einzelnen Teilnehmern und Leitungen im Kommunikationssystem eine VBZ-Gruppe zu. Beim Kodieren der Verbindungsmatrix können Sie dann auf diese Gruppen zurückgreifen und festlegen, welche Teilnehmer welche anderen Teilnehmer erreichen können und welche Teilnehmer auf welche Leitungen zugreifen können.

Standardmäßig sind alle Teilnehmer und Amtsleitungen der VBZ-Gruppe 1 zugeordnet. Damit haben alle Teilnehmer uneingeschränkten Zugang zu anderen Teilnehmer sowie zu Leitungen, sowohl kommend als auch gehend. Welche VBZ-Gruppen Verbindungen zu welchen anderen VBZ-Gruppen herstellen können, ist in der VBZ-Matrix festzulegen.

Es sind maximal 64 VBZ-Gruppen konfigurierbar.

15.1.5.2 Zuordnung der KWZ-Nummern zu VBZ-Gruppen

Jeder VBZ-Gruppe wird ein Bereich von zentralen Kurzwahlzielen (KWZ-Zielen) zugeordnet. Wählt ein Teilnehmer eine KWZ, wird anhand der zugehörigen VBZ-Gruppe geprüft, ob er hierzu berechtigt ist. Liegt diese KWZ im zugeordneten Bereich KWZ für die entsprechende VBZ-Gruppe, wird die Wahl ausgeführt, ansonsten erfolgt eine Fehlermeldung.

Wählt ein Teilnehmer ein Kurzwahlziel, wird die dazugehörige VBZ-Gruppe ermittelt. Daraus leitet sich ab, ob der Teilnehmer dazu berechtigt ist, dieses

Kurzwahlziel zu wählen. Bei fehlender Berechtigung wird die Wahl mit einer Fehlermeldung abgewiesen

Die Kurzwahlziel-Bereiche können sich in den VBZ-Gruppen überschneiden.

Standardmäßig sind alle Kurzwahlziel-Nummern der VBZ-Gruppe 1 zugeordnet.

Die KWZ-Bereiche können sich in den VBZ-Gruppen überschneiden. Zulässig sind z. B.:

VBZ-Gruppe	KWZ-Bereich
1	0000-7999
2	0050-0150
3	0200-0500

Es ist jedoch nicht zulässig, in einer VBZ-Gruppe anstelle eines Bereichs einzelne KWZ oder mehrere KWZ-Bereiche einzutragen. Unzulässig sind z. B.:

VBZ-Gruppe	KWZ-Bereich
1	0000, 0005, 0010
2	0050-0100, 0300-0500

15.1.5.3 Wie Sie Teilnehmer einer VBZ-Gruppe zuweisen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Berechtigungen**.

3) Klicken Sie im Menübaum auf **Berechtigungen > VBZ-Gruppenzuordnung > VBZ-Gruppenzuordnung**.

4) Wählen Sie für einen in der Spalte **Teilnehmer** angezeigten Teilnehmer in der Aufklappliste **Gruppe** den Eintrag mit der gewünschten Verkehrsbeziehungs-gruppe.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

15.1.5.4 Wie Sie die Leitung einer VBZ-Gruppe zuweisen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Berechtigungen**.
3) Klicken Sie im Menübaum auf **Berechtigungen > VBZ-Gruppenzuordnung > Zuordnung Leitung zu VBZ-Gruppe**.
4) Wählen Sie für eine in der Spalte **Leitungen** angezeigte Leitung in der Aufklappliste **Gruppe** den Eintrag mit der gewünschten Verkehrsbeziehungsgruppe.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

15.1.5.5 Wie Sie die VBZ-Matrix ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Berechtigungen**.
3) Klicken Sie im Menübaum auf **Berechtigungen > VBZ-Matrix**.
4) Ändern Sie die Verbindungsmöglichkeiten wie folgt:
   - Wenn Sie alle Verbindungsmöglichkeiten sperren möchten, klicken Sie auf **Alles Sperren**.
   - Wenn Sie alle Verbindungsmöglichkeiten freigeben möchten, klicken Sie auf **Alles Freigeben**.
   - Wenn Sie nur gruppeninterne Verbindungsmöglichkeiten freigeben möchten, klicken Sie auf **Nur Gruppenintern**.
   - Wenn Sie eine Verbindungsmöglichkeit zwischen zwei VBZ-Gruppen gezielt bearbeiten möchten, klicken Sie in das Feld am Kreuzungspunkt dieser VBZ-Gruppen in der VBZ-Matrix. Klicken Sie wiederholt in das Feld, um Verbindungsmöglichkeiten in die eine Richtung, in die andere Richtung oder in beide Richtungen freizugeben oder zu sperren.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

15.1.6 Zentrales Codeschloss, Berechtigungsumschaltung

Das zentrale Codeschloss ermöglicht eine weitgehende Sperre der Telefonfunktionen durch einen berechtigten Teilnehmer (evtl. Administrator) für einen anderen Teilnehmer. Nur folgende Leistungsmerkmale stehen dann noch zur Verfügung: interne Anrufe, Kurzwahl zentral und Konferenz mit internen Teilnehmern. Dieses Codeschloss kann der gesperrte Teilnehmer durch Eingabe

seines Telefonschloss-Codes oder wiederum der berechtigte Teilnehmer deaktivieren.

Der Telefonschloss-Code des Telefons, für den das Codeschloss vom berechtigten Teilnehmer aktiviert oder deaktiviert werden soll, ist für eine Sperrung nicht erforderlich.

Der berechtigte Teilnehmer ist standardmäßig der Teilnehmer mit der Rufnummer "100" (umkonfiguriert).

15.1.7 Individuelles Codeschloss (Telefon abschließen)

Mit dem Individuellen Codeschloss wird erreicht, dass von diesem Telefon aus keine externen Gespräche geführt oder Benutzereinstellungen geändert werden können.

Notrufnummern können trotz abgeschlossenem Telefon gewählt werden.

Interne Gespräche sind weiterhin möglich.

Ein Weiterverbinden von kommenden Rufen zu internen Teilnehmern ist möglich.

Bei abgeschlossenem Telefon sind nur noch Leistungsmerkmale möglich, die kein externes Wählen erfordern. Die Ausnahme ist das Leistungsmerkmal Kurzwahl zentral.

Als Erinnerung, dass dieses Telefon abgeschlossen ist, erhält der Teilnehmer einen Dauerton (Sonderwählton). Bei Telefonen mit Display wird dem Teilnehmer außerdem im Display "Telefon aufschliessen" angezeigt.

Ein Teilnehmer kann sein Telefon über eine Taste oder Kennzahl durch Eingabe seines persönlichen Telefonschloss-Codes abschließen und auch wieder entsperren.

Vor der ersten Nutzung des Telefonschlosses ist der Telefonschloss-Code zu konfigurieren. Der Telefonschloss-Code wird für alle Telefone standardmäßig auf 00000 gesetzt und kann individuell geändert werden. Dafür muss das Telefon aber entsperrt sein. Der Telefonschloss-Code muss immer 5stellig sein. Es sind nur die Ziffern 0 bis 9 zulässig. Wenn der Teilnehmer den Telefonschloss-Code vergessen hat, kann er durch einen berechtigten Teilnehmer (1. Teilnehmer im System mit der Rufnummer "100" oder der Administrator) auf den Standardwert 00000 zurückgesetzt werden.

15.1.7.1 Wie Sie das individuelle Codeschloss zurücksetzen

Über den Wizard **Teilnehmername und Freischaltung** kann das individuelle Codeschloss eines Telefons zurückgesetzt werden.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards > User-Telefonie**.
3) Klicken Sie auf **Bearbeiten** um den Wizard **Teilnehmername und Freischaltung** zu starten. Das Fenster **Teilnehmer Name und Freischaltung** wird angezeigt.
4) Aktivieren Sie das Kontrollkästchen **Codeschloss zurücksetzen**.
5) Klicken Sie auf **OK & Weiter** und abschließend auf **Beenden**.

15.1.8 R-Gesprächsschutz je Amtsleitung (nur für Brasilien)

R-Gesprächsschutz je Amtsleitung ermöglicht das automatische Auslösen ankommender R-Gespräche. Dieses Leistungsmerkmal ist ausschließlich in der Ländereinstellung Brasilien verfügbar. In allen anderen Ländern wird die Einstellung ignoriert.

Die individuelle Konfiguration für jede analoge Amtsleitung ist möglich. R-Gesprächsschutz kann individuell für jede analoge Amtsleitung konfiguriert werden. Ist das Leistungsmerkmal für eine Amtsleitung freigegeben, wird 1 s (Defaultwert) nach Annahme eines kommenden Rufs die Schleife für 2 s (Defaultwert) geöffnet. Dadurch werden R-Gespräche im Netz ausgelöst, andere Gespräche bleiben unverändert bestehen.

15.1.9 R-Gesprächsschutz je Teilnehmer (nur für Brasilien)

Mit dem R-Gesprächsschutz je Teilnehmer kann für jeden Teilnehmer individuell ein R-Gesprächsschutz eingerichtet und damit ankommende R-Gespräche automatisch ausgelöst werden. Dies gilt auch im Fall einer Anrufumleitung, einer Anrufübernahme, eines Abwurfs usw.

Zusätzlich besteht die Möglichkeit einen systemweiten R-Gesprächsschutz einzustellen. Dieser kommt zum Tragen, wenn kein einzelner Teilnehmer angewählt wird, sondern beispielsweise ein Sammelanschluss (oder bei Falschwahl).

15.2 LCR (Least Cost Routing, Leitweglenkung)

Durch die Funktion Leitweglenkung (LCR Least Cost Routing) wird automatisch gesteuert, über welchen Weg eine gehende Verbindung geschaltet wird. Der Weg kann über das öffentliche Netz, unterschiedliche Netzanbieter (ITSP) oder über ein privates Netz erfolgen. Anhand von Wahlplan, Wegetabellen und Wahlregeln wird der am besten geeignete Verbindungsweg für das Gespräch gesucht.

Mögliche Verbindungen sind Gesprächsverbindungen, analoge Datenverbindungen über Fax und Modem und ISDN-Datenverbindungen.

15.2.1 LCR-Funktionalität

Mit Hilfe der Funktion LCR legen Sie fest, über welchen Anbieter z. B. ein Ortsgespräch, ein Handygespräch oder Auslandsgespräche geführt werden. Sie legen über das Kommunikationssystem den kostengünstigsten Anbieter fest und führen alle entsprechenden Gespräche über diesen definierten Weg.

Wird im Wahlplan ein Muster gefunden, das mit der gewählten Rufnummer übereinstimmt, wird in den Wegetabellen nach einer passenden Richtung gesucht (Jeder Leitung ist eine Richtung zugeordnet. Siehe *Amtszugang über digitale und analoge Leitungen*). Dabei wird überprüft, ob die LCR-Berechtigung für diesen Wegetabelleneintrag zutrifft. Die LCR-Berechtigung und der Unterschied zur Berechtigung (Wahlkontrolle) wird im Kapitel LCR-Berechtigung beschriebenen.

Über die LCR-Funktionalität kann gesteuert werden, welche Teilnehmer des Kommunikationssystems welche Richtungen bzw. Leitungen nutzen dürfen (z. B. um sicherzustellen, dass Faxe ausschließlich über TDM-Amtsleitungen und nicht über ITSP geführt werden). Geprüft wird auch, ob der Anrufer die erforderlich Berechtigung gemäß Wahlkontrolle zur Belegung der gerade von LCR betrachteten Richtung hat. Diese Prüfung ist für Querverkehr (PABX Leitungen) per Konfiguration abschaltbar.

Die gewählten Zeichen werden zwischengespeichert bis die Wegetabellen mit den LCR-Berechtigungen durchlaufen sind. Erst danach erfolgt der Aufbau der Verbindung unter Berücksichtigung der Wahlregeln. Um die Wahlbereitschaft zu signalisieren kann dem Teilnehmer ein Wählton eingeblendet werden.

Sie können bei der Konfiguration der Wahlregeln eine Information für den wählenden Teilnehmer eingeben, z. B. dass diese Verbindung über einen bestimmten Telefondienstanbieter (Angabe des Providers) geroutet wird oder es sich bei einer Verbindung um eine teure Verbindung handelt. Diese Information kann entweder im Display angezeigt werden, als Ton ausgegeben oder im Display und gleichzeitig als Ton ausgegeben werden.

Generell gilt:

- Wenn LCR aktiviert ist, wird die Prüfung für jede externe Wahl durchgeführt. Ausnahme: bei gezielter Wahl einer Leitungskennzahl bzw. Leitungstaste.
- Wenn LCR feststellt, dass die bevorzugte Leitung nicht genutzt werden kann, so sucht das Kommunikationssystem eine alternative (möglicherweise teuerere) Richtung aus der Wegetabelle aus.
- Ziffern können je nach Zugangsverfahren und je Wegetabelle einzeln oder blockweise übertragen werden.
- Wenn die Durchwahlnummerntabelle leer ist, wird ersatzweise die Tabelle der internen Rufnummern verwendet. Es gelten die entsprechenden Regeln für diese Tabelle.

INFO: Auch bei Kommunikationssystemen mit analogen Amtsleitungen (HKZ) muss eine Standortnummer konfiguriert werden

(Ländervorwahl / ggf. Ortsnetzkennzahl / ggf. Anlagenrufnummer).

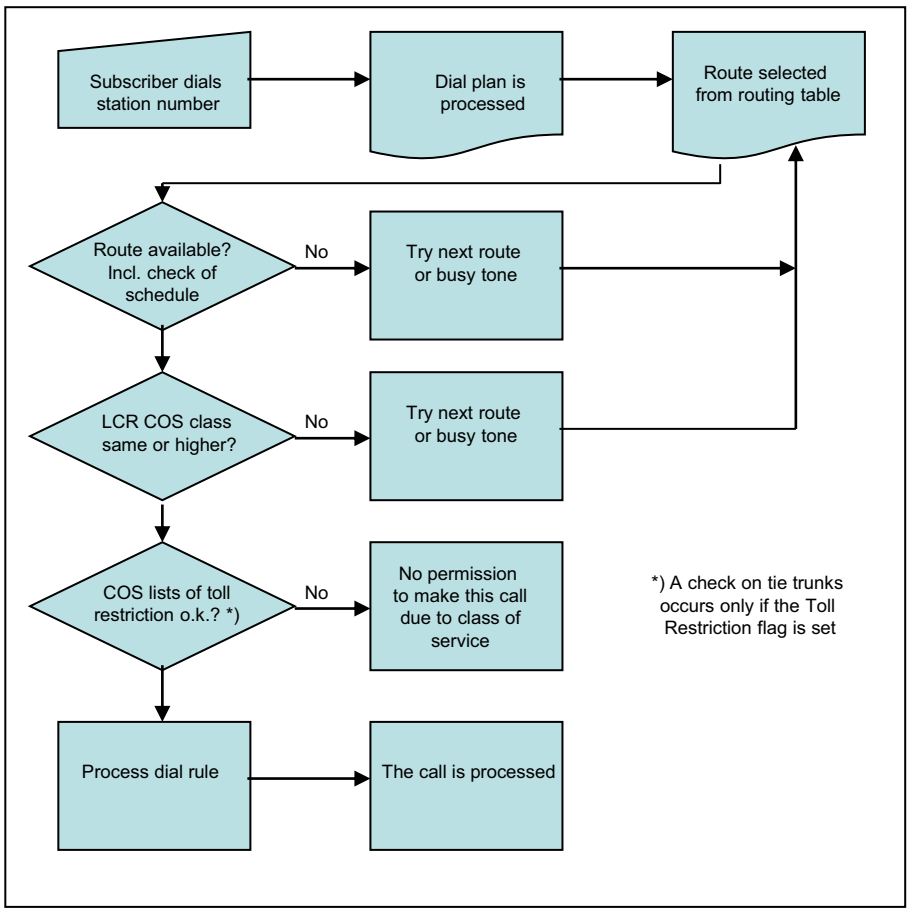
Darüber hinaus muss eine Durchwahlnummer oder, im Falle eine leeren Durchwahlnummerntabelle, eine Durchwahlnummer des eigenen analogen Amtsanschlusses (HKZ) konfiguriert werden. Nur so ist sichergestellt, dass alle externen Ziele erreicht werden können.

Systemspezifische Informationen

Das Kommunikationssystem wertet insgesamt 24 Zeichen aus.

Das Kommunikationssystem kann bis zu 1000 Wahlpläne und 254 Wegetabellen, mit je 16 Einträgen, verwalten.

LCR-Flußdiagramm



Wahlaussendung

Bei der Wahlaussendung wird zwischen Schritthaltend und Blockweise unterschieden. Bei Schritthaltend wird jede Ziffer direkt nach der Wahl ausgesendet und verarbeitet (Voraussetzung: LCR-Bewertung ist komplett, d. h. Wahlplaneintrag ist eindeutig identifiziert und Berechtigungen sind geprüft). Bei Blockwahl

werden Ziffernblöcke gebildet und gesendet (d. h. Leitungsbelegung und Wahl erfolgen erst nach Zeit bzw. bei vorhandener expliziter Wahlendekennung).

Die Wahlaussendung für ITSP-Richtungen muss immer blockweise erfolgen. Die Einstellung der Richtung ist für die gesamte Wegetabelle wirksam.

Nur für USA: Carrier Select Override

Carrier Select Override kann mittels gezielter Leitungsbelegung realisiert werden (Kennzahl, Taste). Der LCR-Mechanismus wird dabei komplett umgangen.

Abhängigkeiten

Thema	Abhängigkeit
Zeitplan	Wenn in einem von HiPath 3000 migrierten System eine LCR-Konfiguration mit Zeitplan vorliegt, sind diese Einträge weiterhin wirksam und können mit dem Manager E administriert werden.
Kurzwahl zentral	Damit zentrale Kurzwahlziele ordnungsgemäß funktionieren, muss im Kurzwahlziel die LCR-Zugangskennziffer, gefolgt von der Zielrufnummer eingetragen sein.
Namentasten	Namentasten für externe Ziele müssen mit der LCR-Zugangskennziffer programmiert sein, damit sie ordnungsgemäß funktionieren.
Berechtigung (Wahlkontrolle)	Die Berechtigungsklassen der Wahlkontrolle werden auch bei LCR angewendet. Für PBX-Leitungen kann die Wahlkontrolle abgeschaltet werden, die Konfiguration erfolgt durch ein Flag.
Prime Line	Wenn die "Automatische Leitungsbelegung" (Prime Line) zum Amt aktiviert ist, dann ist LCR nicht möglich. Diese beiden Leistungsmerkmale schließen sich gegenseitig aus.

15.2.1.1 Wie Sie die LCR freigeben

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

> ***INFO:*** Bestimmte Einträge wie z. B. Ortsnetzkennzahl oder Teilnehmernummer werden bereits im Wizard **Basisinstallation** vorgenommen. Manuelle Änderungen dieser Einträge sind nur durch geschultes Techniker auszuführen. Bei Fehlkonfiguration im LCR besteht die Gefahr, dass gehende Verbindungen nicht oder nur eingeschränkt möglich sind.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > LCR**.

3) Klicken Sie auf die Registerkarte **LCR Flags** ändern.

4) Aktivieren Sie das Kontrollkästchen **LCR freigeben**.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**

15.2.2 LCR-Wahlplan

Im Wahlplan wird nach Mustern gesucht, die auf die gewählten Ziffern (Wählfolge) zutreffen. Das Ergebnis dient als Kriterium für die Auswahl der Wegetabelle. Dabei wird überprüft, ob die LCR-Berechtigung des Teilnehmers für diesen Wahlplaneintrag zutrifft.

Das Muster einer Wählfolge ist im Wahlplan einer Wegetabelle zugeordnet, die weitern Parameter für diesen Verbindungaufbau definiert.

Der Wahlplan wird für Identifizierungs- und Konfigurationszwecke in einzelne Felder gegliedert. Die Tabelle stellt die Nummern 4922000 und 1603656260 bei Eingabe in den Wahlplan dar.

Feld 1	Feld 2	Feld 3	Feld 4	Feld 5
0 C	492	– 2000		
0 C	160	– 365	– 62	– 60

Für die Rufnummern sind folgende Einträge gültig:

0 . . . 9	Erlaubte Ziffern
–	Feldtrennzeichen
C	Simulierter Wählton (kann max. dreimal eingetragen werden). Dieser Eintrag wird auch als Feldtrennzeichen interpretiert
Globalzeichen	
X	Beliebige Ziffer zwischen 0 . . . 9
N	Beliebige Ziffer zwischen 2 . . . 9
Z	Eine oder mehrere Ziffern folgen bis Wahlende

Eine Ziffernfolge kann in maximal 10 Felder unterteilt werden.

Feldtrennzeichen dienen der Unterteilung der Ziffernfolge in einzelne, getrennt auswertbare Felder. Beispiel: Nach der ersten Wählziffer wird ein Feldtrennzeichen eingefügt, damit eine gewählte “0” als separates Feld erkannt wird und somit eine Amtsberechtigung simuliert.

Durch die Trennung der Felder, können diese Felder im Wahlplan wiederholt bzw. anders angeordnet werden. Die durch die Feldtrennzeichen “–” und “C” gebil-

deten Felder im Wahlplan können einzeln angesteuert werden, um Ziffern zu wiederholen, zu unterdrücken, auszutauschen oder einzufügen.

Ein "#"- oder "*"-Zeichen in der vom Teilnehmer gewählten Ziffernfolge bezeichnen das Wahlende bzw. die Umschaltung des Wahlverfahrens. Aus diesem Grund sind diese Zeichen keine gültigen Einträge im Wahlplan.

Einträge mit Globalzeichen müssen immer durch eine eindeutige Wahlziffer eingeleitet werden, um Konflikte zwischen verschiedenen Globalzeicheneinträgen zu vermeiden.

Die PKZ-Eingabe kann pro Wahlplan erzwungen werden. Dabei gilt das PKZ-Prüfverfahren.

Wenn zu einem Wahlstring mehrere Wahlplaneinträge passen, wird der am meisten übereinstimmende verwendet. Beispiel: 00894711 wird gewählt, Wahlplaneinträge 0CZ und 0C089Z sind vorhanden -> 0C089Z wird ausgeführt. Die Position der Einträge innerhalb des Wahlplans ist irrelevant, es ist kein "sortierter" Eintrag erforderlich.

OpenScape Business kann eine Wählfolge bis zu einer Länge von 24 Zeichen auswerten.

LCR-Einträge bei Ersteinrichtung des Kommunikationssystems

Bei der erstmaligen Inbetriebnahme des Kommunikationssystem erfolgen länderabhängig bestimmte Defaulteinträge im LCR-Wahlplan. Bis Wahlplan 34 werden systemseitige Einträge für Notrufe, Auskunft, Sonderrufnummern, Standard-Amtsbelegung für PSTN und ITSP, für UC Suite, Ansageanschalten und Networking und die Berücksichtigung der Wahl im internationalen Format auf ISDN-Amtsleitungen vorbelegt. Dieser Bereich kann durch Konfigurationsänderungen an anderer Stelle (z. B. Änderung des Flags **Standortnummer**) beeinflusst werden. Es ist daher sicherzustellen, dass die Standard-Amtsbelegung mit einer Änderung der Standortnummer weiterhin funktioniert (dies ist wichtig bei Wahl mit öffentlichen Rufnummern).

INFO: Ab LCR-Wahlplan 36 stehen Einträge zur freien Verfügung.

15.2.2.1 Wie Sie den Wahlplan bearbeiten

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > LCR**.

3) Klicken Sie auf **Wahlplan**.

4) Unter **Wahlplan ändern** werden die einzelnen Wahlpläne aufgelistet und Sie können folgende Felder bearbeiten:

- **Name**
- **Gewählte Ziffern**
- **Wegetabelle**
- **PKZ**
- **Wahlkontrolle**

  Das Flag Wahlkontrolle bezieht sich ausschließlich auf die Richtungsart PABX. Für die Richtung Amt hat es keine Bedeutung, d. h. es ist nicht möglich die Wahlkontrolle für Amtsleitungen an dieser Stelle auszuschalten.
- **Notbetrieb**

INFO: Durch Klicken auf den blauen Pfeil neben dem Feld **Wegetabelle** öffnet sich direkt die zugehörige Wegetabelle.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**

15.2.3 LCR-Wegetabelle

In den Wegetabellen der Leitweglenkung LCR wird nach einer passenden Richtung gesucht (jeder Leitung muss eineRichtung zugeordnet sein). Dabei wird überprüft, ob die Berechtigung (Wahlkontrolle) für diese Richtung zutrifft. Vom zugewiesenen Weg ist auch die Wahlregel abhängig.

Die Wegetabelle beschreibt

- die dem betreffenden Weg zugewiesene Richtung,
- die Wahlregel,
- die für eine Belegung erforderliche LCR-Berechtigung,
- die Möglichkeit zur Warnung vor einer teuereren Verbindung (Warnsignal).
- das dedizierte Gateway und
- die GW Knoten-ID.

Die Tabelle wird von oben nach unten in hierarchischer Reihenfolge durchsucht. Es wird jeweils überprüft, ob die Richtung frei ist bzw. der Teilnehmer die erforderliche LCR-Berechtigung hat. Ist dies der Fall, erfolgt die Wahl gemäß der in der Wegetabelle eingetragenen Wahlregel, wenn die Berechtigung (Wahlkontrolle) und die VBZ-Zuordnung zwischen Teilnehmer und Leitung das zulassen.?

Wenn der primäre Verbindungsweg in der Wegetabelle belegt ist, kann LCR den nächsten (möglicherweise kostspieligeren) in der Tabelle konfigurierten Weg wählen. Dies kann dem Anwender durch ein akustisches und/oder optisches Signal angezeigt werden.

Es können bis zu 254 Wegetabellen mit jeweils 16 Wegen angelegt werden.

Dediziertes Gateway

Ein dediziertes Gateway ist in einem IP-Netzverbund ein fest eingestellter Partnerknoten (Dediziertes Gateway -> erzwungen). Wenn ein Dediziertes Gateway mit der entsprechenden GW Knoten-ID für die IP-Netorking-Richtung eingetragen ist, so wird zwingend zu diesem Gateway geroutet.

Bei einer Multigateway-Konfiguration wird ein Dediziertes Gateway anhand der Teilnehmerkonfiguration ermittelt.

15.2.3.1 Wie Sie Wegetabellen bearbeiten

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > LCR**.

3) Klicken Sie auf **Wegetabelle**.

4) Alle Wegetabellen werden Ihnen angezeigt:

- **1-Table**
- **2-Table**
- **nn-Table**

INFO: Die Wegetabellen 1 bis 15 sind für Default-Enträge bzw. für eine Konfiguration über Wizards vorgesehen. Bei einer Migration werden automatisch die vorhandenen Einträge in diese Wegetabellen eingetragen.

Dieser Mechanismus verhindert allerdings keine Duplikate bei den Einträgen. Eine manuelle Nachbearbeitung der Wegetabellen wird empfohlen.

---

5) Klicken Sie auf die gewünschte Wegetabelle. Die ausgewählte Tabelle mit der Registerkarte **Wegetabelle ändern** wird angezeigt.

6) Unter **Wegetabelle ändern** werden die einzelnen Wegetabellen aufgelistet und Sie können folgende Felder bearbeiten:

- **Richtung**
- **Wahlregel**
- **min. Ber. (LCR-Berechtigung)**
- **Warnung**
- **Dediziertes Gateway**
- **GW Knoten-ID**

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

15.2.4 LCR-Berechtigung

Jedem Teilnehmer wird eine eigene LCR-Berechtigung zugewiesen. Ein Teilnehmer kann einen Weg nur dann belegen, wenn seine Berechtigung größer oder gleich der LCR-Berechtigung in der Wegetabelle ist, das heißt ein Teilnehmer mit Berechtigung 7 kann einen Weg mit Berechtigung 8 nicht belegen. Standardmäßig sind alle Teilnehmer mit maximaler LCR-Berechtigung (15) eingetragen.

Abhängigkeiten

Thema	Abhängigkeit
Wahlkontrolle	Die Berechtigungen (Wahlkontrolle) ist vorrangig vor der LCR-Berechtigung. Die Berechtigung (Wahlkontrolle) kann für Querleitungen ein- und ausgeschaltet werden.
VBZ-Zuordnung	Eine Wahl erfolgt nur, wenn auch die VBZ-Matrix dies zulässt.

15.2.4.1 Wie Sie die LCR-Berechtigung vergeben und ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > LCR**.

3) Klicken Sie auf **Classes of Service**.

4) Vergeben Sie unter **Berechtigungen ändern** im Feld **Berechtigung** eine LCR-Berechtigung bzw. ändern eine vorhandene Berechtigung.

Hierbei handelt es sich ausschließlich um die Berechtigung eines Teilnehmers für LCR. Das Feld hat keinen Einfluss auf die Amtsberechtigung.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

15.2.5 LCR-Wahlregeln

Durch die LCR-Wahlregeln können eingegebene Rufnummern zur Weiterverarbeitung in beliebige neue Ziffernfolgen umgewandelt werden. Durch Ziffernumwandlung wird der Zugang zu verschiedenen Netzanbietern ermöglicht. Die

verwendete Wahlregel wird bestimmt durch den Weg bzw. die Richtung in der Wegetabelle.

Systemspezifische Informationen

Das Kommunikationssystem ist in der Lage bis zu 254 Wahlregeln in der LCR-Wahlregeltabelle zu verwalten. Der Name einer Wahlregel kann bis zu 16 Zeichen umfassen.

Die Regeln sprechen die einzelnen Felder im Wahlplan für nachstehende Vorgänge selektiv an:

- Wiederholen von Ziffern
- Unterdrücken von Ziffern
- Austauschen von Ziffern
- Einfügen von Ziffern
- Umschalten des Wahlverfahrens
- Erkennen eines Wähltons
- Einfügen von Wahlpausen

Wahlregel

Sie können hier bis zu 254 Wahlregeln mit einer Länge von jeweils maximal 40 Zeichen definieren.

Die LCR-Wahlregeltabelle wird auch als Routingtabelle bezeichnet.

Definition der Wahlregeln (Wahlregelformat)

- A:
  Restliche Felder wiederholen (aussenden). "A" bewirkt, dass alle nachfolgenden Ziffernfelder gesendet werden. Bezugspunkt ist das letzte Feldtrennzeichen im Feld gewählte Ziffern im Wahlplan.
  Wird "A" ohne expliziten Bezug eingetragen, bezeichnet dies alle Ziffern nach dem Acces Code, d. h, "A" entspricht dann "E2A"?
- B:
  Wird für die Multi-Gateway-Vernetzung genutzt, wenn eine von extern angerufene Rufnummer vom TON (Type Of Number) "unknown" ist, um sie zum Multi-Gateway-Knoten zu routen. Damit diese Rufnummer eindeutig ist, wird sie entsprechend der TON im LCR auf national oder international erweitert. Dies ist erforderlich, wenn die Durchwahlnummern nicht eindeutig sind und ins nationale oder internationale Format konfiguriert werden müssen.
- D (n):
  Ziffernfolge wählen (1 bis 25 Ziffern). "D" darf in der Zeichenkette mehrmals vorkommen und an beliebigen Stellen stehen.
- E (n):
  Aussenden des Feldinhaltes (1 bis 10). "E" darf in der Zeichenkette mehrmals vorkommen und an beliebigen Stellen stehen. Die Reihenfolge von "E" in Abhängigkeit von (n) ist beliebig. Ein bestimmtes Feld darf mehrmals, auch

aufeinanderfolgend, angesprochen werden. "E" darf mit Ausnahme von "E1" (Access Code) von beliebigen anderen Parametern eingeschlossen sein Bei schritthaltender Wahl (Gegensatz zur Blockwahl) darf das letzte Element in der Wahlregel nicht E(n) heißen, sondern E(n)A.

- M (n):
  Autorisierungscode (1 bis 16). Dieser Buchstabe darf nicht an der letzten Stelle stehen.
- P (n):
  Pause, "P" darf in der Zeichenkette mehrmals vorkommen und an beliebigen Stellen stehen.
- S:
  Switch, Umschalten des Wahlverfahrens von IWV auf MFV (bei CONNECT, PROGRESS oder CALL PROC mit PI). "S" darf in der Zeichenkette nur einmal vorkommen und darf nicht an der letzten Stelle stehen. Nach "S" darf nicht mehr der Parameter "C" verwendet werden.
- C:
  Carrier "C" darf in der Zeichenkette nur einmal vorkommen. Die nachfolgenden Zeichen werden ohne Wahlpause gesendet und für den Carrierzugang bei "Single Stage", "Two Stage", "DICS" und "PRI" verwendet.
- U:
  Anwenden des Wahlverfahrens SUB-Adresse. "U" darf in der Zeichenkette nur einmal vorkommen und darf nicht an der letzten Stelle stehen. Nach "U" dürfen die Parameter "S", "P" "M" und "C" nicht mehr verwendet werden.
- N (n) (Nur für USA!):
  Netz-SFG-Gruppe (1 bis 5) oder Bandnummer (1).
- L (Nur für USA!):
  "L" darf nur am Ende der Zeichenkette vorkommen. "L" bewirkt, dass der Anruf als Notruf behandelt wird.

Beispiel:

Das System soll automatisch eine Providervorwahl voranstellen.

Wahlregel D010xxA bedeutet: das System wählt zunächst die Provider-Vorwahl (010xx), dann alle Ziffern nach dem Access Code, die der Teilnehmer gewählt hat (A).

15.2.5.1 Wie Sie Wahlregeln bearbeiten

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > LCR**.

3) Klicken Sie auf **Wahlregel**. Alle Wahlregeln werden Ihnen angezeigt.

4) Klicken Sie auf die gewünschte Wahlregel im Menübaum.

5) Sie können folgende Felder bearbeiten:

- **Regelname**
- **Wahlregelformat**
- **Verfahren des Netzanbieters** (**Unbekannt**, **Hauptnetzanbieter**, **MCL Single Stage**, **MCL Two Stage**, **Corporate Network**, **Dial In Control Server**, **Primary Rate Interface**)
- **Type** (**Unbekannt**, **Ländervorwahl**, **Ortnetzvorwahl**, **Anlagenrufnummer**)

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

15.2.6 Netzanbieter

Netzanbieter können mit jeder Richtung verbunden werden. Die Auswahl des jeweiligen Netzanbieters wird durch die Wahlregeln für LCR definiert.

Unbekannt

Keine explizite Angabe über einen Netzanbieter.

Hauptnetzanbieter

Bei einer Belegung über den Hauptnetzanbieter erfolgt die einfache Wahl durch Blockwahl oder Wahl einzelner Ziffern in das öffentliche Netz.

MCL Single Stage

Bei MCL Single Stage wird mit einem Präfix der gewünschte Netzanbieter angewählt und anschließend die Rufnummer gewählt. Die Wahl erfolgt dabei bei ISDN im D-Kanal bzw. als normale Wahl bei HKZ.

MCL Two Stage

Bei MCL Two Stage wird mit einem Präfix der gewünschte Netzanbieter angewählt. Nach einer Synchronisationsphase wird zunächst ein ebenfalls konfigurierbarer Authorisierungscode und darauffolgend die Ziel-Rufnummer als DTMF-Zeichen gesendet

Bei Synchronisation durch Zeit muss eine Pause von 2 bis 12 s programmiert werden.

Corporate Network

Ein Corporate Network ist direkt am Kommunikationssystem angeschlossen. Die LCR-Funktion bestimmt aus der vom Teilnehmer gewählten Nummer die entsprechende Richtung und routet das Gespräch entweder über das Leitungsbündel des öffentliches Amtes oder über das Leitungsbündel mit dem firmeneigenen Netz.

Dial In Control Server

Bei dieser Art LCR wird mit einem Präfix der gewünschte Netzanbieter über einen Dial-In Control Server (DICS) angewählt und dabei die Rufnummer und ein konfigurierbarer Authorisierungscode in der Subadresse übermittelt. Die Wahl erfolgt dabei im D-Kanal.

Primary Rate Interface (Primärmultiplexschnittstelle) (nur für USA)

Beim Primary Rate Interface erfolgt die Auswahl des Netzanbieters bzw. des Calling Service in der SETUP-Meldung über die Informationselemente Network Specific Facility, Operator System Access und Transit Network Selection.

Abhängigkeiten

Thema	Abhängigkeit
Anrufinformationen erhalten/weitergeben	Temporäre oder permanente Rufnummernunterdrückung darf nicht aktiviert sein.
ISDN/SUB-Addressing	Das ISDN-Leistungsmerkmal "SUB" muss im öffentlichen Netz beantragt bzw. freigegeben sein.

15.2.7 Gezielte Belegung von Amtsleitungen

Amtsleitungen können von Teilnehmern gezielt belegt werden.

Normalerweise ist eine Priorisierung für die Amtsholung über Least Cost Routing vorgegeben. Meistens ist dabei der günstigste Anbieter an erster Stelle, der zweitgünstigste an zweiter Stelle usw.

Möchte ein Teilnehmer ein Gespräch über einen Anbieter, der nicht an erster Stelle geroutet wird, führen (weil dieser z. B. für Ferngespräche noch günstiger ist), so kann er diesen Anbieter gezielt über eine Leitungs-Kennzahl oder über eine Leitungstaste anwählen.

Ebenso hat der Teilnehmer über die gezielte Wahl per Kennzahl die Möglichkeit eine Rufnummer zu wählen, deren Wahl nur über ISDN möglich ist (sollte als Anbieter ansonsten z. B. Vodafone vorgegeben sein).

Standardmäßig wird eine Kennzahl (88) für eine gezielte Amtsbelegung über ISDN eingerichtet. Alle Kennzahlen können vom Administrator nachträglich eingericht bzw. geändert werden.

15.2.7.1 Wie Sie die Kennzahl für gezielte Belegung von ISDN-Amtsleitungen konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > LCR**.

3) Klicken Sie auf **Wahlplan**. Die einzelnen Wahlpläne werden aufgelistet.

4) Geben Sie unter **Name** den gewünschten Namen für den Wahlplan ein.

5) Geben Sie unter **Gewählte Ziffern** die Kennzahl und die Kürzel exakt ein (z. B. **88CZ**).

> ***INFO:*** 88 ist die standardmäßig vom System vergebene Kennzahl für die gezielte Belegung einer ISDN-Amtsleitung.
> Informationen zu den Kürzeln C und Z siehe *LCR-Wahlplan*.

6) Geben Sie unter **Wegetabelle** eine **1** ein.

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

15.2.7.2 Wie Sie Kennzahlen für die gezielte Amtsbelegung anzeigen

Mit dem Wizard **Amtsleitung ISDN / Analog / ITSP** können Sie die Kennzahlen für die gezielte ISDN-Amtsbelegung anzeigen lassen.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.
- Das Kommunikationssystem ist an eine analoge Amtsleitung angeschlossen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Zentrale Telefonie**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Amtsleitung ISDN / Analog / ITSP** zu starten.

4) Klicken Sie so oft auf **OK & Weiter** bis Sie zum Fenster **Kennzahlen für die gezielte Amtsbelegung** kommen.

5) Im Default sehen Sie die Kennzahl für die gezielte ISDN-Amtsbelegung. Bei konfigurierten ITSPs werden die entsprechenden Kennzahlen angezeigt.

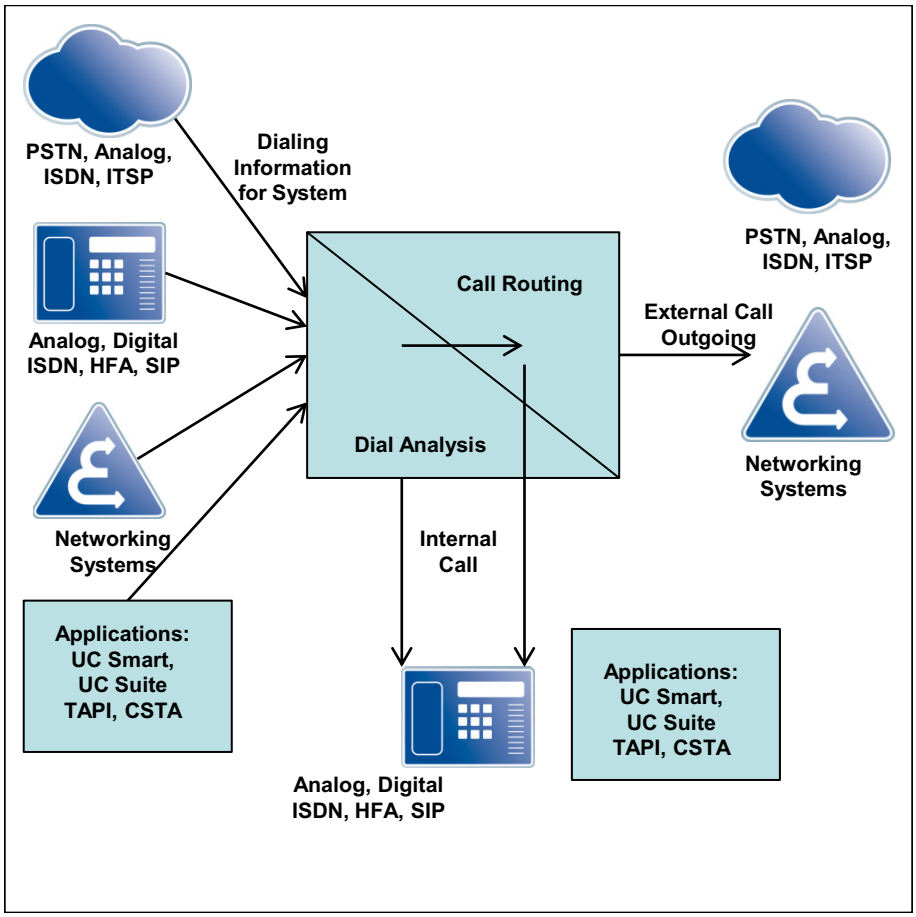
6) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

15.3 Wahlbewertung und Call-Routing

In diesem Kapitel wird der Zusammenhang zwischen Wahlbewertung und Call-Routing verdeutlicht. Es erklärt wie das Kommunikationssystem Rufnummern bewertet, die durch Teilnehmer, Leitungen und Applikationen unterschiedlicher Art zur Anwahl eines beliebigen Ziels gewählt werden und wie das Routing nach abgeschlossener Wahlbewertung erfolgt. Die hierfür relevanten Systemfunktionen wurden zum großen Teil bereits in den vorherigen Kapiteln beschrieben. Die Wahl mit öffentlicher Rufnummer innerhalb eines Knotens/einer Vernetzung wird in diesem Abschnitt detailliert beschrieben.

Die Wahlbewertung

- des Kommunikationssystems erfasst und bewertet alle gewählten Rufnummern anhand der Konfigurationsdaten
- prüft Berechtigungen. (z. B. anhand von Berechtigungsklassen für Teilnehmer, Teilnehmerflags, Tag/Nacht, erlaubte und verbotene Rufnummern, LCR-Berechtigungen, Zeitplänen, Verbindungsmatrixen, etc.).
- entscheidet, ob eine gewählte Rufnummer intern zugestellt wird oder eine Leitung zu belegen ist. Das gilt sowohl für die Wahl von Internrufnummern als auch für Öffentliche Rufnummern, als auch für netzinterne Rufnummern.
- normiert Rufnummern, d. h. macht Rufnummern für das Kommunikationssystem wählbar. (z.B. kanonisches Format wird von "+49nnn" zu "00049nnn")
- kürzt ggf. Rufnummern (führende Ziffern von Zielrufnummern bei kommender Amtsbelegung werden ggf. abgeschnitten, um DID-Ziele im kurzen Format zu ermitteln)



15.3.1 Überblick Call Routing / LCR

Ein eingehender Anruf wird im Kommunikationssystem verschiedenen Prüfungen unterzogen und entsprechend weitergeleitet.

Prüfung 1 (Internes Rufziel?)

- Ziele mit kanonischer Rufnummer werden zunächst in wählbare Rufnummern (an der Teilnehmer-Schnittstelle) gewandelt, bzw. mit TON=International versehen (ITSP-Schnittstelle).
- Zielrufnummern von Leitung werden ggf. um den Rufnummernanteil der Anlagenrufnummer der entsprechenden Richtung gekürzt.
- Internrufe werden über den internen Wahlplan bewertet, Rufe von Extern durch den Wahlplan der Durchwahlrufnummern.

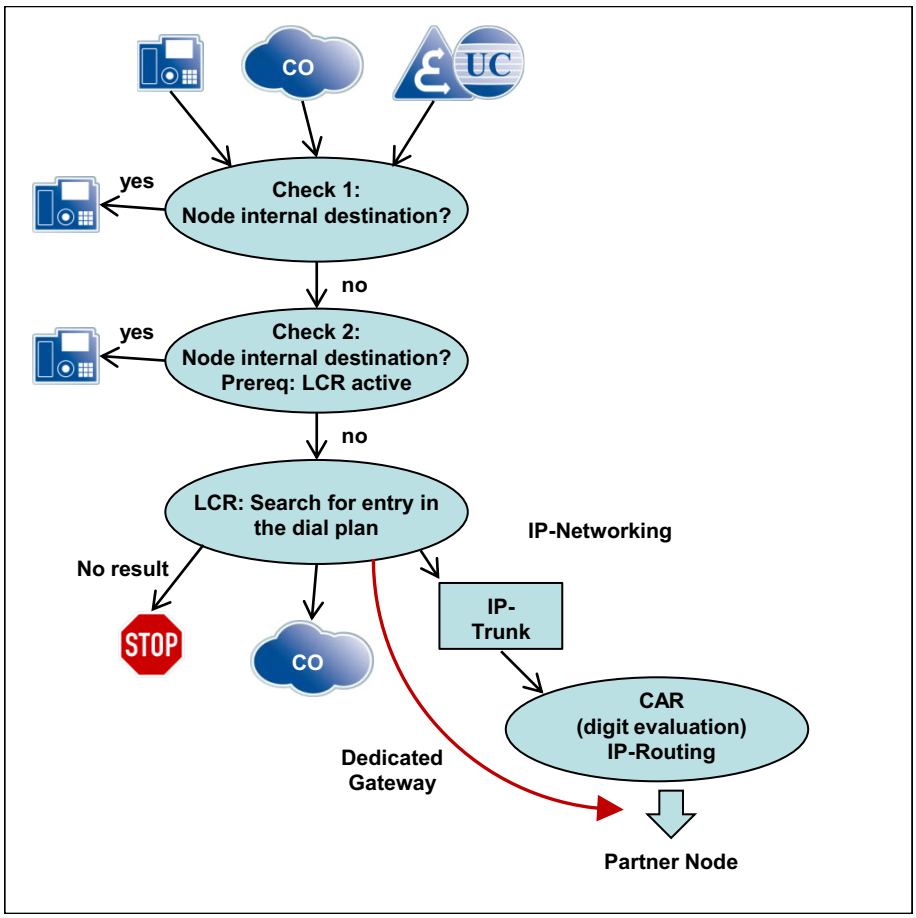
Prüfung 2 (Internes Rufziel?)

- Teilnehmer, Applikationen, Clients oder andere Kommunikationssysteme wählen Zielrufnummern im öffentlichen Format (z. B. 0 0049nnn)
- Bedingung: Standard-Amtskennzahl (z. B. "0") ist eingerichtet
- Zielrufnunmmer wird entsprechend der Anteile der Standortrufnummer (Gateway Standort) gekürzt und anhand des Wahlplans der Durchwahlruf-

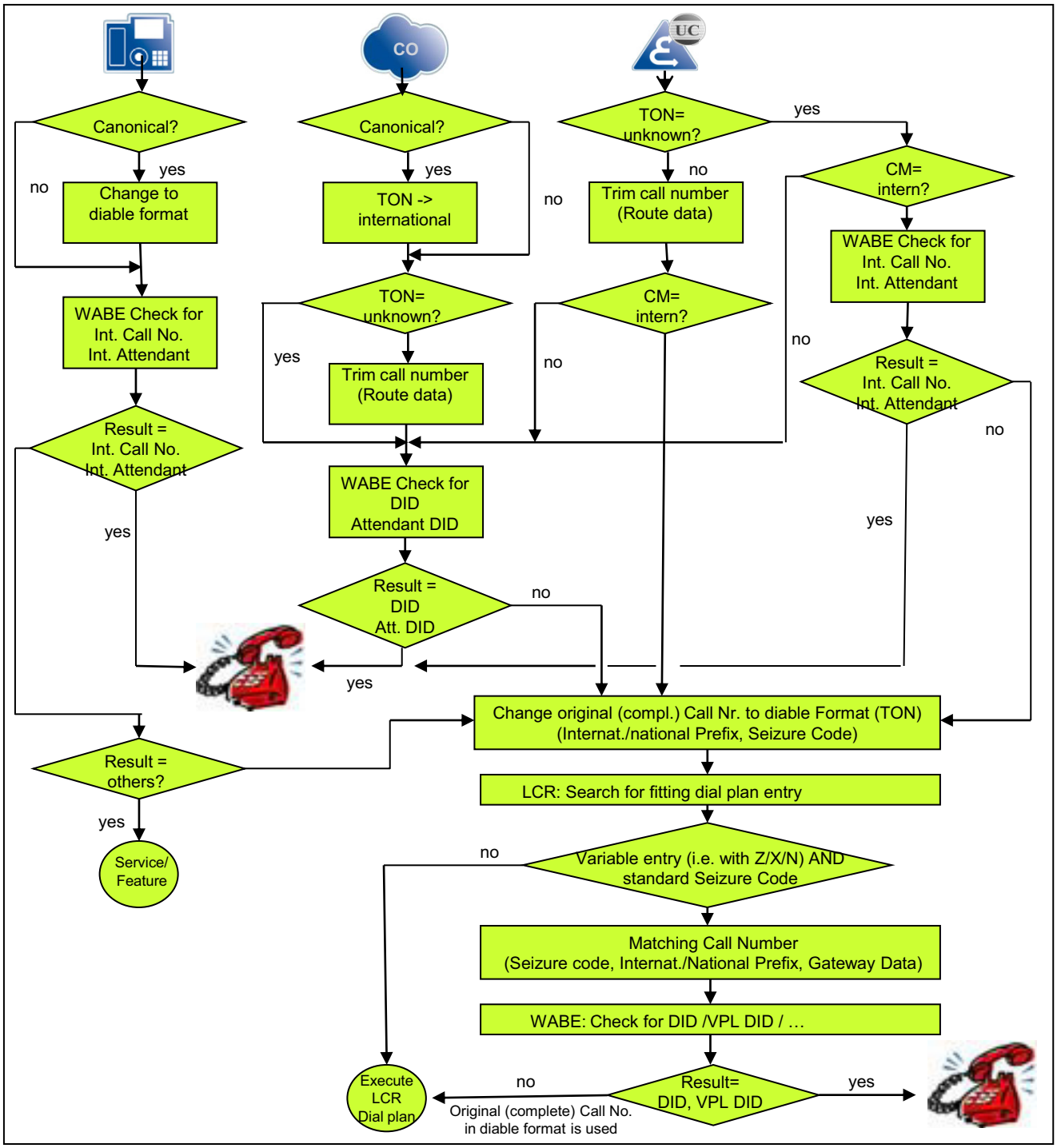
nummern bewertet, unabhängig davon, ob es sich um einen Intern- oder Externruf handelt.

- Falls kein internes Rufziel gefunden wird, wird die wählbare, ungekürzte (!) Rufnummer im LCR verarbeitet und der Anruf entsprechend über eine Leitung weitergeroutet.

Innerhalb einer IP-Vernetzung ermöglicht der LCR-Wegetabelle-Parameter "Dedicated Gateway" die direkte Adressierung eines Knotens für eine gewählte Rufnummer unter Umgehung der CAR-Wahlbewertung.



15.3.2 Flußdiagramm Wahlbewertung



Erläuterungen zum Flußdiagramm:

Deutsch	Englisch	Erläuterung
WABE		Wahlbewertung
CM	CM	Classmark, kennzeichnet den Anrufer als externen oder (netz-)internen Anrufer
TON	TON	Type Of Number Rufnummerntyp: Unknown, Subscriber (Teilnehmer), National oder International und wird sowohl bei Zielrufnummern als auch bei Ursprungsrufnummern verwendet.
DuWa	DID	Durchwahlrufnummer
TNR RNR	Int. Call No.	Internrufnummer
Int. Attendant	VPL INT	Vermittlungsplatznummer für Interanrufe
VPL DID	VPL DID	Vermittlungsplatznummer für Externanrufe
SERVICE	SERVICE	Servicekennzahl
LCR	LCR	Least Cost Routing

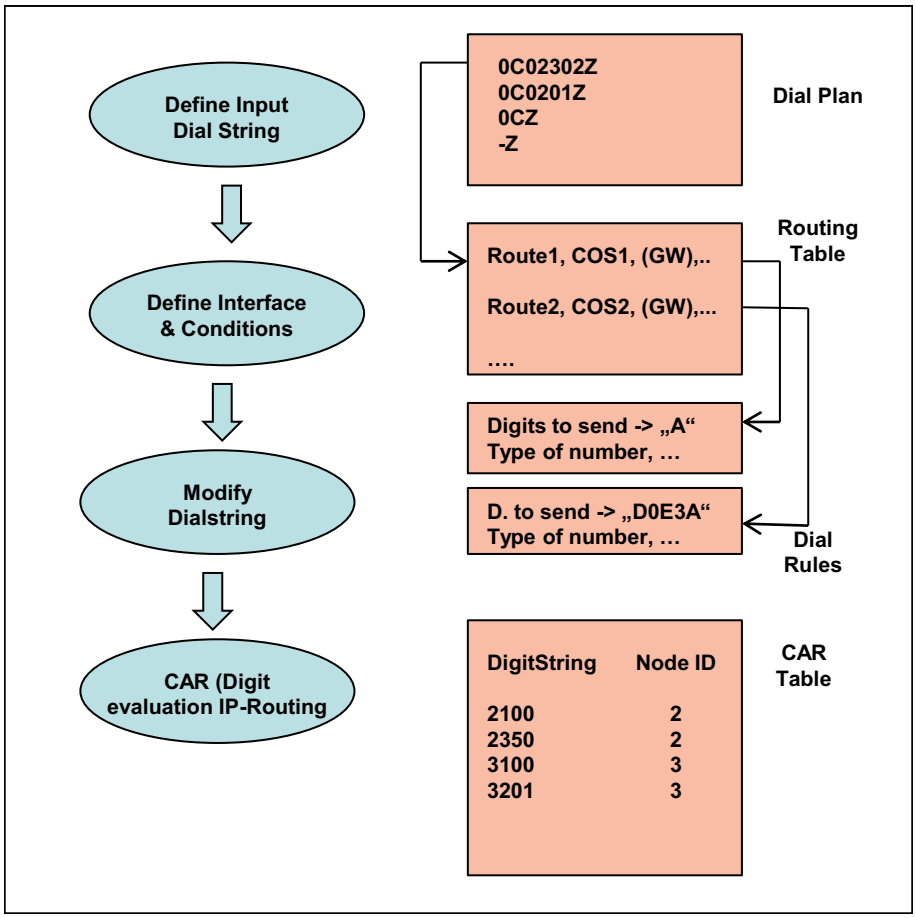
UC Clients verhalten sich bzgl. der Wahlbewertung wie Teilnehmer, die über CSTA gesteuert werden.

Die UC Suite verhält sich bzgl. der Wahlbewertung wie ein SIP-Q-Trunk.

15.3.3 Call Routing und LCR im Netzverbund

Bei der Vernetzung spielen Call Routing und LCR eine wichtige Rolle. Über Wahlplan und Wahlregeln werden die Anrufe geroutet. Eine besondere Rolle übernimmt das dedizierte Gateway.

LCR Basics



Die Einträge in der Wegetabelle (Routing table) werden, wenn keine erfolgreiche Leitungsbelegung erfolgt, nacheinander in einer Schleife abgearbeitet.

LCR-Einträge bei der Ersteinrichtung

Bei der erstmaligen Inbetriebnahme des Kommunikationssystem erfolgen länderabhängig bestimmte Default-Einträge im LCR-Wahlplan. Bis Wahlplan 35 werden systemseitige Einträge für Notrufe, Auskunft, Sonderrufnummern, Standard-Amtsbelegung für PSTN und ITSPs, UC Suite, Vernetzung und die Berücksichtigung der Wahl im internationen Format auf ISDN-Amtsleitungen vorbelegt.

Dieser Bereich kann durch Konfigurationsänderungen (z. B. Änderungen des Flags **Standortnummer**) beeinflusst werden. Daher ist sicherzustellen, dass die Standard-Amtsbelegung mit der Änderung der Standortnummer weiterhin funktioniert (wichtig bei Wahl mit öffentlichen Rufnummern).

INFO: Ab LCR-Wahlplan 36 stehen Einträge zur freien Verfügung.

15.3.3.1 Dediziertes Gateway

Das dedizierte Gateway ist nur bei einer IP-Vernetzung relevant.

Warum ein dediziertes Gateway notwendig ist?

- Die CAR-Tabelle jedes Kommunikationssystems enthält netzweite Rufnummern der jeweils anderen Knoten und wird zyklisch bei Updates automatisch aktualisiert (überschrieben). Daher sind CAR-Tabellen nicht geeignet um manuell hinzugefügte Einträge dauerhaft zu nutzen.
- Es sind netzweit gültige Rufnummern eingetragen, d. h. es ist kein knotenindividuelles Routing möglich (z. B. "0" zum jeweils zugehörigen Gateway-Knoten)

Wie können Ziele per Konfiguration, dauerhauft eingerichtet werden?

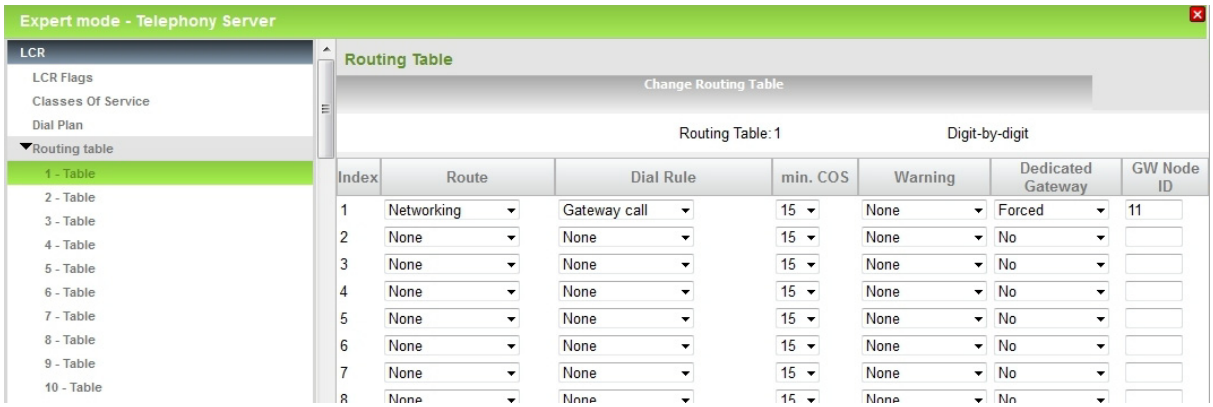
- Durch Verwendung einer direkten Adressierung im LCR
- Das dedizierte Gateway adressiert direkt den Zielknoten anhand der Knoten ID (IP-Adresse)
- Bei Verwendung des dedizierten Gateways werden die CAR-Tabellen übersprungen (siehe vorheriges Bild).

Anwendungsfälle für ein dediziertes Gateway

Direktes Adressieren

- von TDM-Gateways um Amtsleitungen zu belegen ("0CZ")
- von TDM-Gateways um Breakouts über separate Kennzahlen zu realisieren
- von netzinternen Knoten, die über öffentliche Rufnummern erreicht werden sollen
- von TDM-Gateways, denen die Teilnehmer einer Multi Gateway Vernetzung (an einer OpenScape Business S) zugewiesen sind (z. B. Teilnehmer 1 gehört per Definition zum Gateway 1 und Teilnehmer 2 gehört zum Gateway 2).
- von Gateways und Anrufen, deren Urspung in einer Multi Gateway Konfiguration NICHT einem bestimmten Gateway zugeordnet werden können (z. B. die Faxgruppe eines UC Contact Centers)

Das dedizierte Gateway im WBM



Folgende Werte können eingestellt werden:

Nein (No)	Die Rufnummernbewertung erfolgt anhand der CAR-Tabellen (keine **GW Knoten-ID** erforderlich)
Erzwungen (Forced)	Wird direkt zum entsprechenden Gateway geroutet (GW Knoten-ID = n)
Mehrere Standorte (Multi Location)	Nur bei Multi Gateway Konfigurationen zu verwenden: Anhand der Multi Gateway Konfiguration der OpenScape Business S Teilnehmer kennt das Kommunikationssystem die Zuordnung zu deren Gateway und kann daher den gehenden Anruf gezielt zum entsprechenden Gateway routen. In der Konfiguration **Mehrere Standorte** wird die GW Knoten-ID nur dann verwendet, wenn durch die Zuordnung der Teilnehmer kein Gateway identifiziert werden kann (Default).

15.3.4 Szenarien: Wahlbewertung und Call Routing

Anhand von Szenarien werden Abhängigkeiten und erforderliche Konfigurationsparameter beschrieben, um die Abläufe im Kommunikationssystem zu erläutern. Die dargestellten Szenarien können je nach Anwendungsfall aufeinander aufbauen.

Einzelsystem

1. Teilnehmer A ruft Teilnehmer B über Internrufnummer
2. Teilnehmer A ruft Teilnehmer B über öffentliche Rufnummer
3. Teilnehmer A ruft externen Teilnehmer über Amt
4. ISDN Amt ruft Teilnehmer A
5. Sonderkonfigurationen und entsprechende Auswirkungen:
   2 Amtsrichtungen

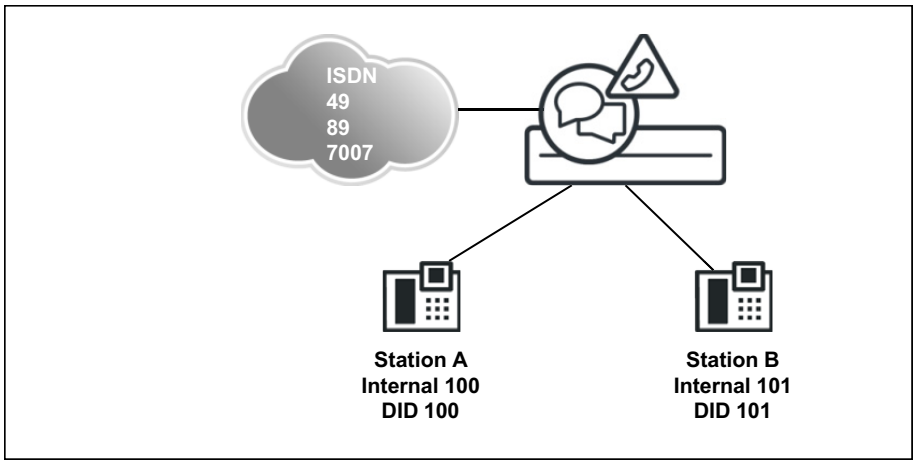
Vernetztes System als Unteranlage (ohne Amtsleitung)

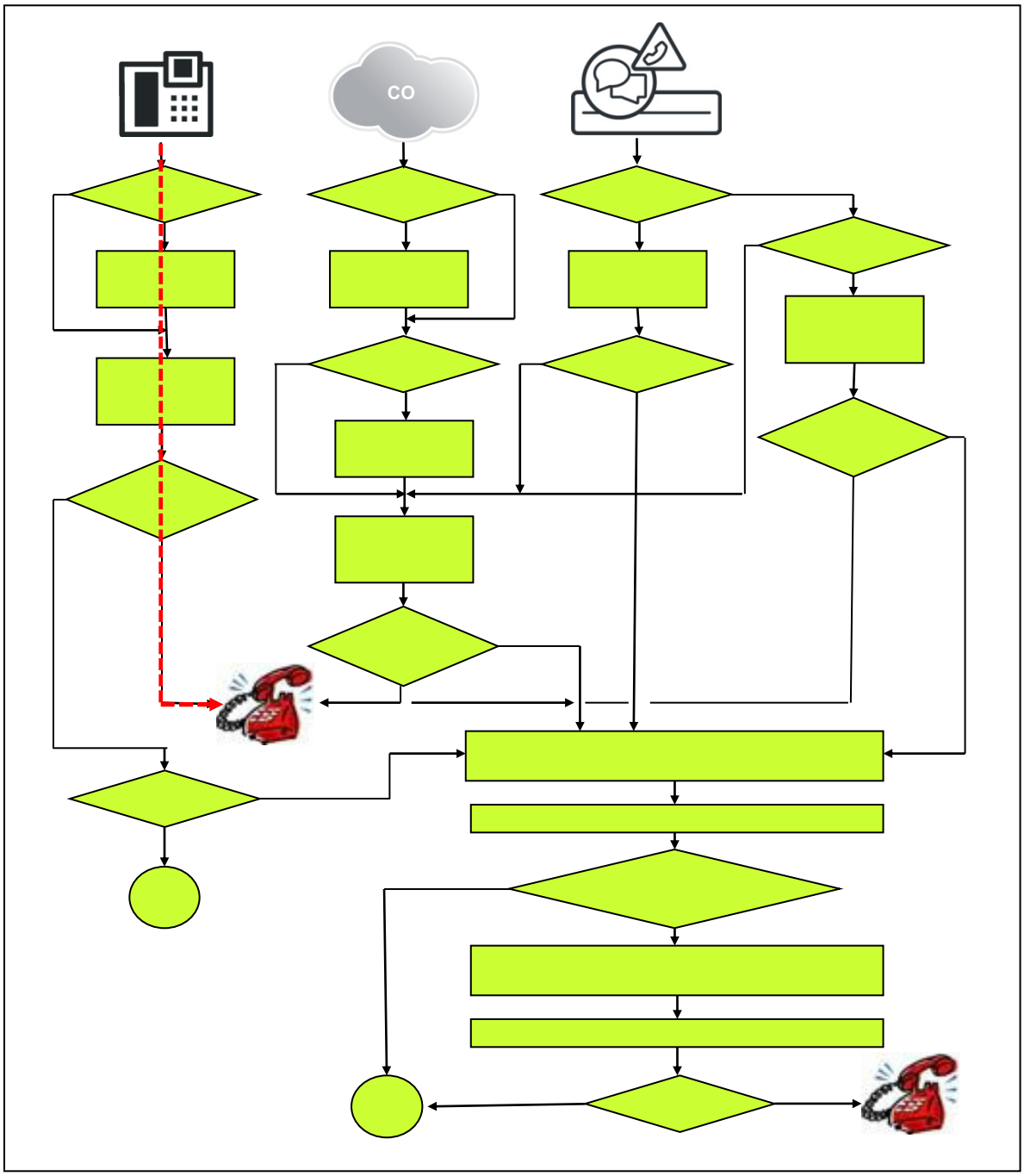
1. Teilnehmer A ruft Teilnehmer C über Internrufnummer
2. Teilnehmer A ruft Teilnehmer C über öffentliche Rufnummer im Netzverbund
3. ISDN Amt ruft Teilnehmer C

Netzverbund mit Multi Gateway

1. ISDN Amt Gateway 1 ruft Teilnehmer D
2. Teilnehmer D ruft externen Teilnehmer über Amt

15.3.4.1 Teilnehmer A ruft Teilnehmer B über Internrufnummer

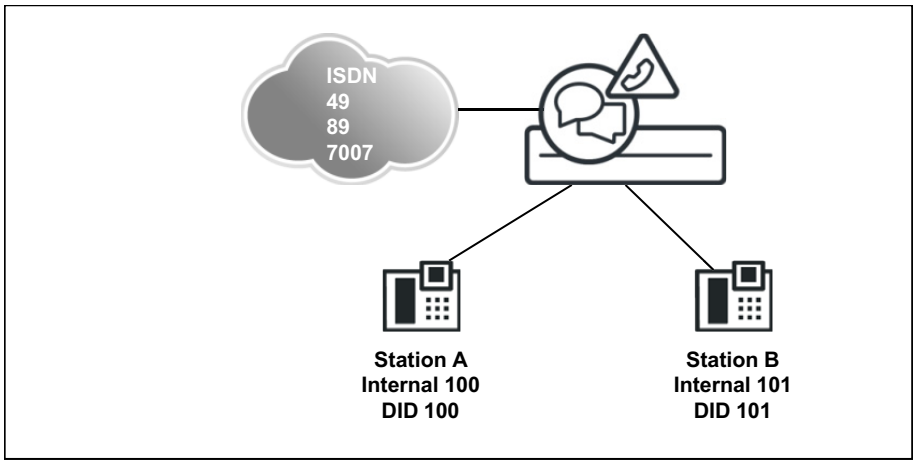




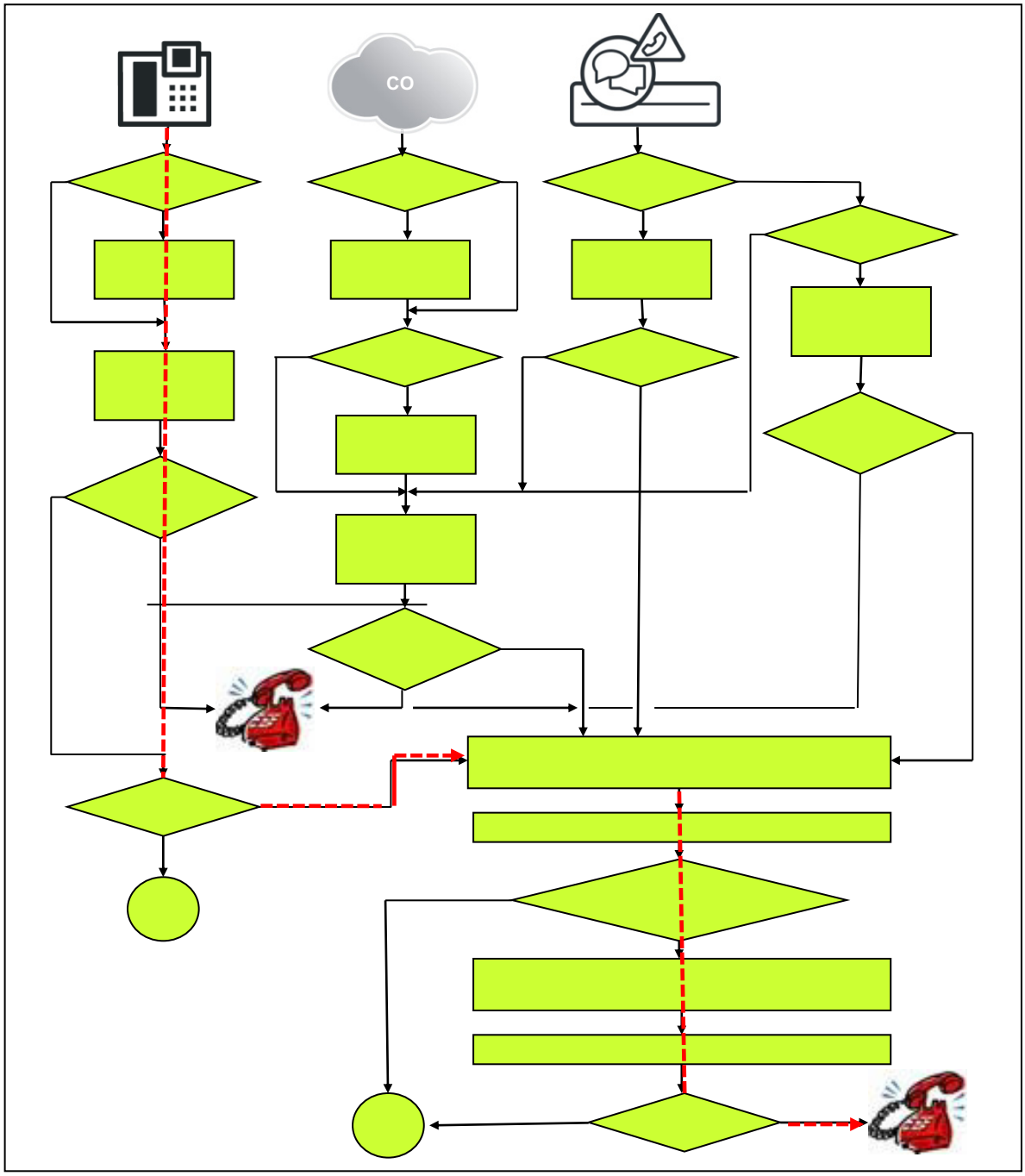
Konfiguration der beiden Intern-Rufnummern

	Box	Slot	CallNo	Name	DID	Type
	1	1	100	-	100	System Client
	1	1	101	-	101	System Client

15.3.4.2 Teilnehmer A ruft Teilnehmer B über öffentliche Rufnummer



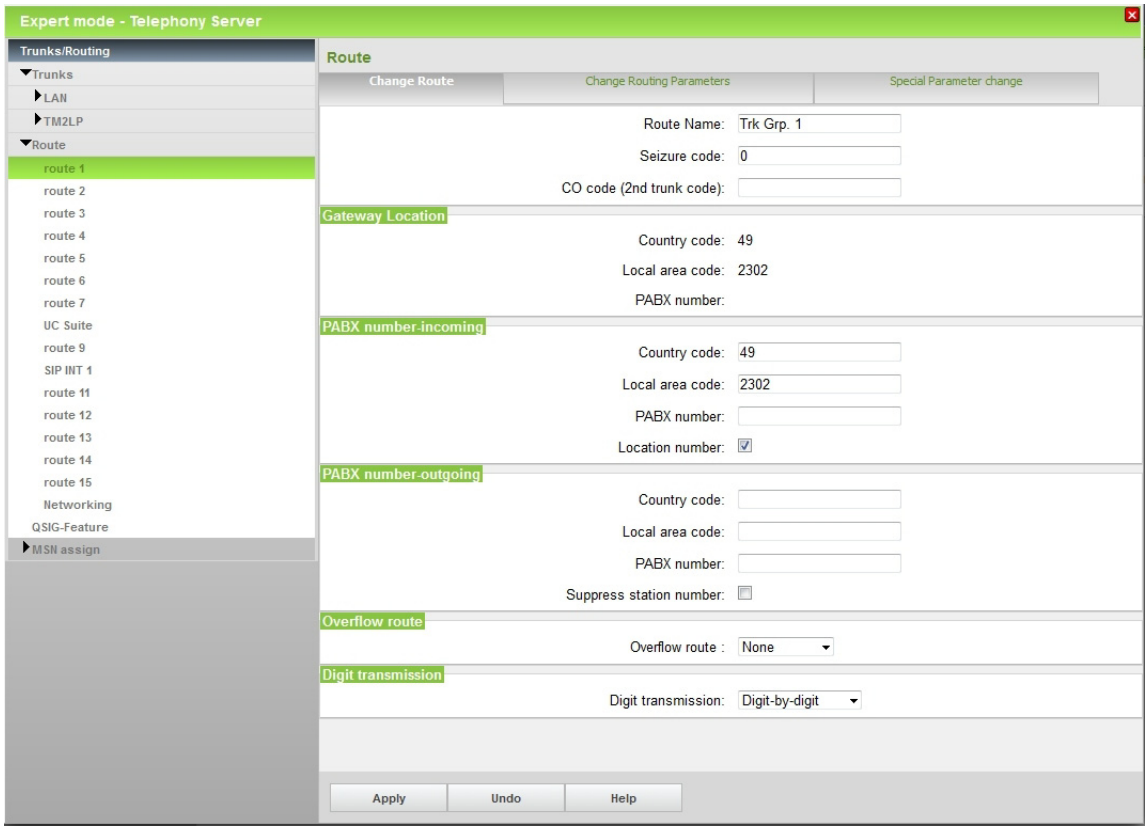
Der Anruf wird system-intern zugestellt, da die Zielrufnummer ein DID-Teilnehmer des eigenen Systems ist.



Konfiguration

	Box	Slot	CallNo	Name	DID	Type
	1	1	100	-	100	System Client
	1	1	101	-	101	System Client

Nachdem die Zielrufnummer anhand der Gateway Location abgestrippt wurde, wird mit der abgestrippten Rufnummer im DID-(DUWA-)Rufnummernplan nach einem Ziel gesucht.



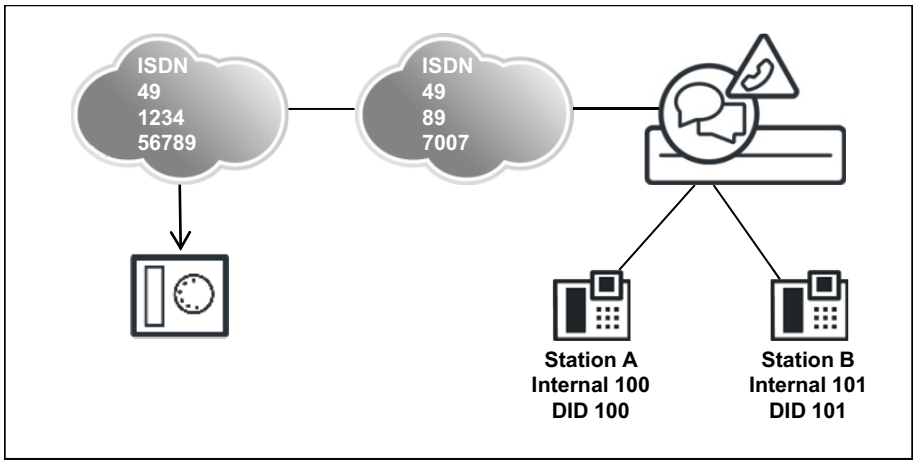
Abhängigkeiten der "Standortnummer" (Gateway Location)

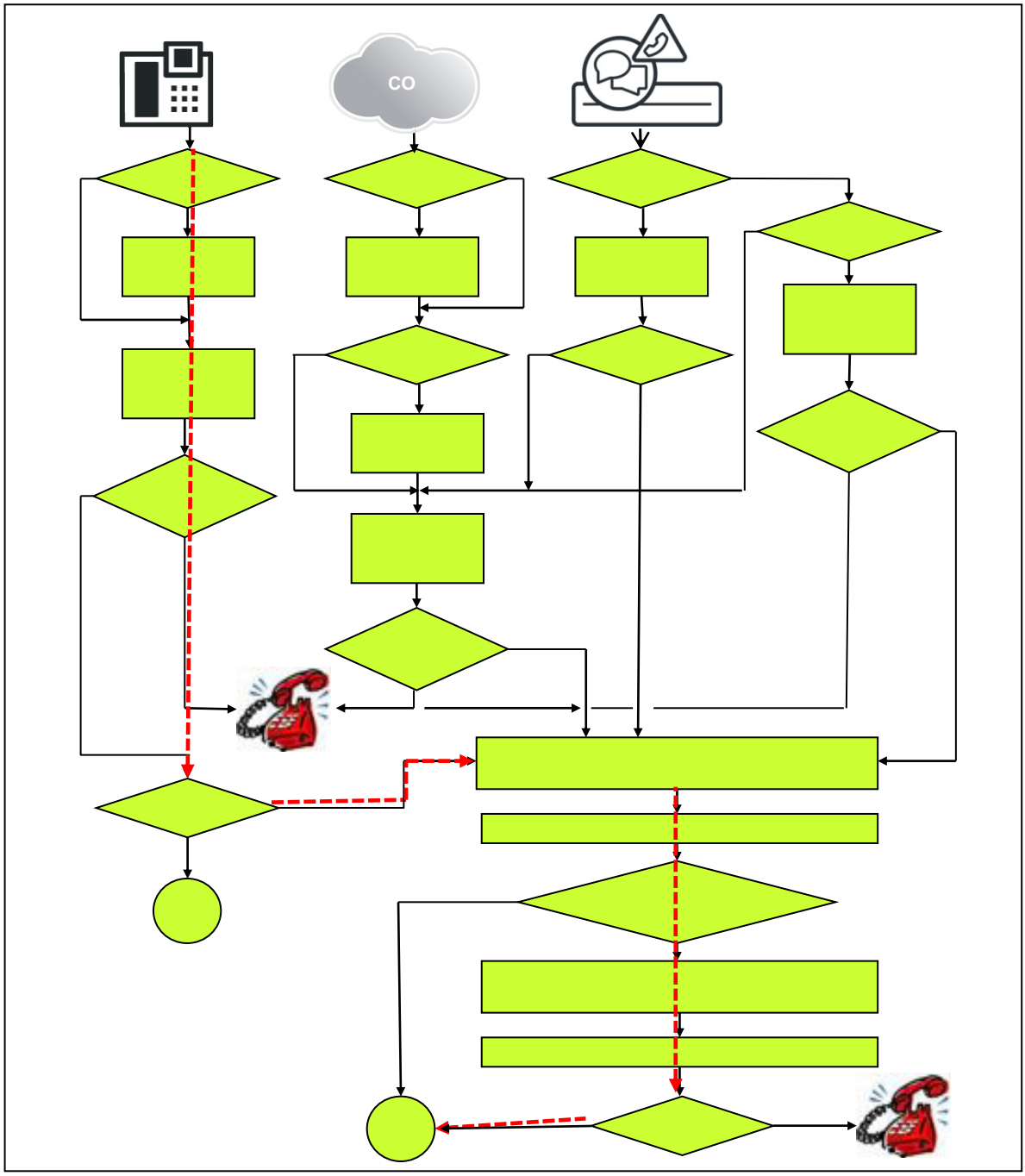
Die Standortnummer (Gateway Location) wird bei der Wahl mittels öffentlicher Rufnummer ausgewertet. Wenn die gewählte Rufnummer in den relevanten Anteilen mit dieser Nummer übereinstimmt, wird die DID-Tabelle ausgewertet und, bei Übereinstimmung, das betreffende interne Ziel gerufen (keine Belegung einer Leitung !). Die Standortdaten werden durch Setzen des Flags Location Number automatisch von den entsprechenden Richtungsdaten (PABX-Number incoming) übernommen und brauchen in Standardszenarien nicht verändert zu werden.

In den DID-Tabellen dürfen daher nur gültige, diesem System zugeordnete Rufnummern eingetragen sein, da sonst Verdeckungseffekte mit Rufnummern im öffentlichen Netz auftreten können. Es würde sonst u. U. das durch eine ungültige DID identifizierte interne Ziel gerufen, obwohl ein Ruf über eine Leitung zu einem externen Ziel beabsichtigt ist.?

Änderungen des Flags "Standortnummer" beeinflussen unter Umständen die vorbelegten Standard-LCR-Einträge. Es ist sicherzustellen, dass die Standard-Amtsbelegung mit der Änderung der Standortnummer weiterhin funktioniert. Dies ist wichtig bei Wahl mit öffentlichen Rufnummern.

15.3.4.3 Teilnehmer A ruft externen Teilnehmer über Amt

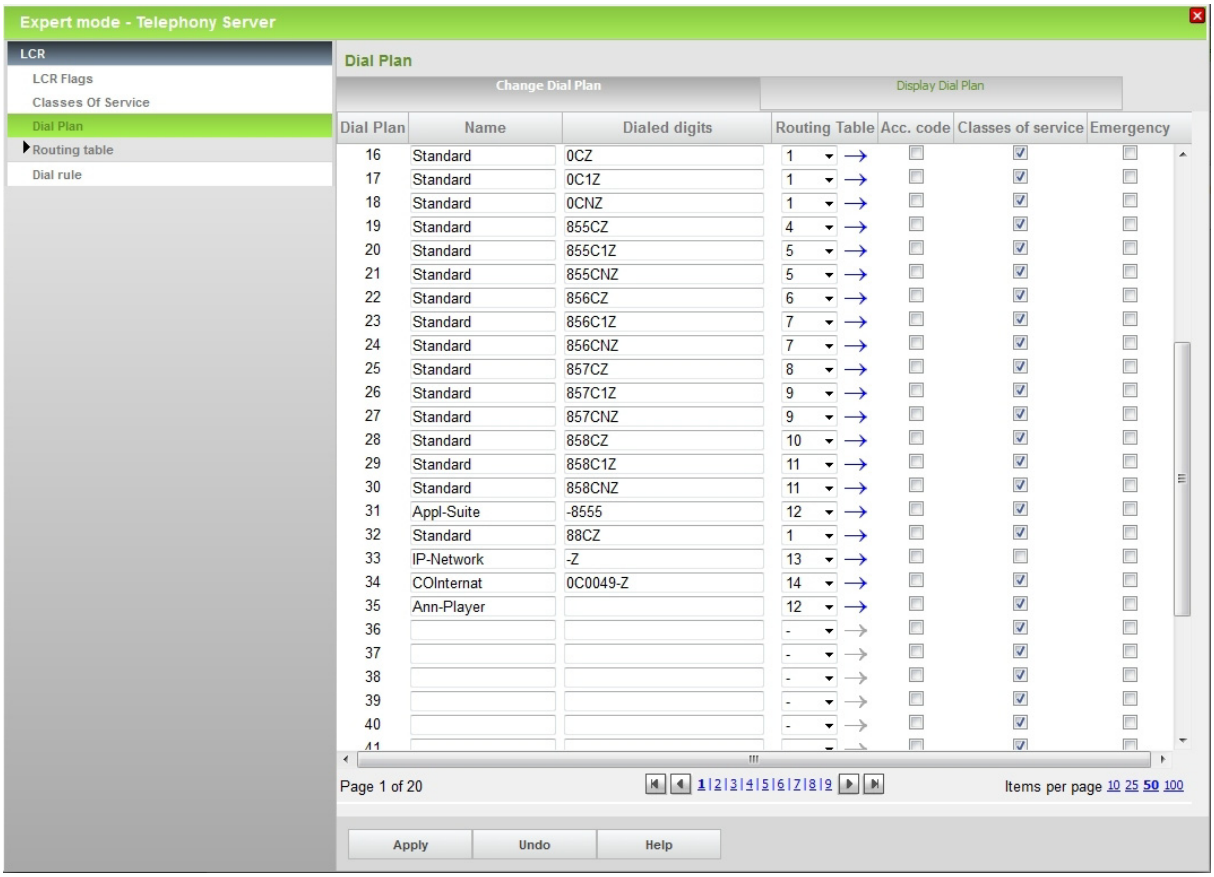




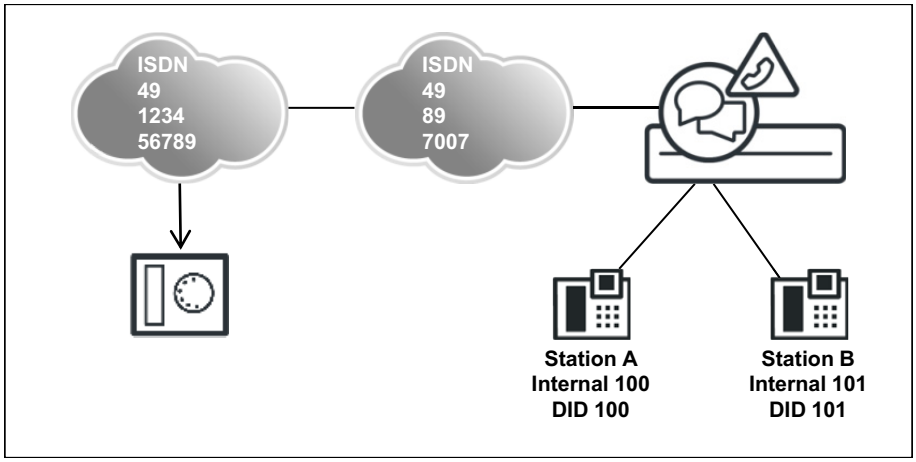
Der Anruf wird per LCR geroutet, da das Ziel nicht im eingenen Kommunikationssystem liegt.

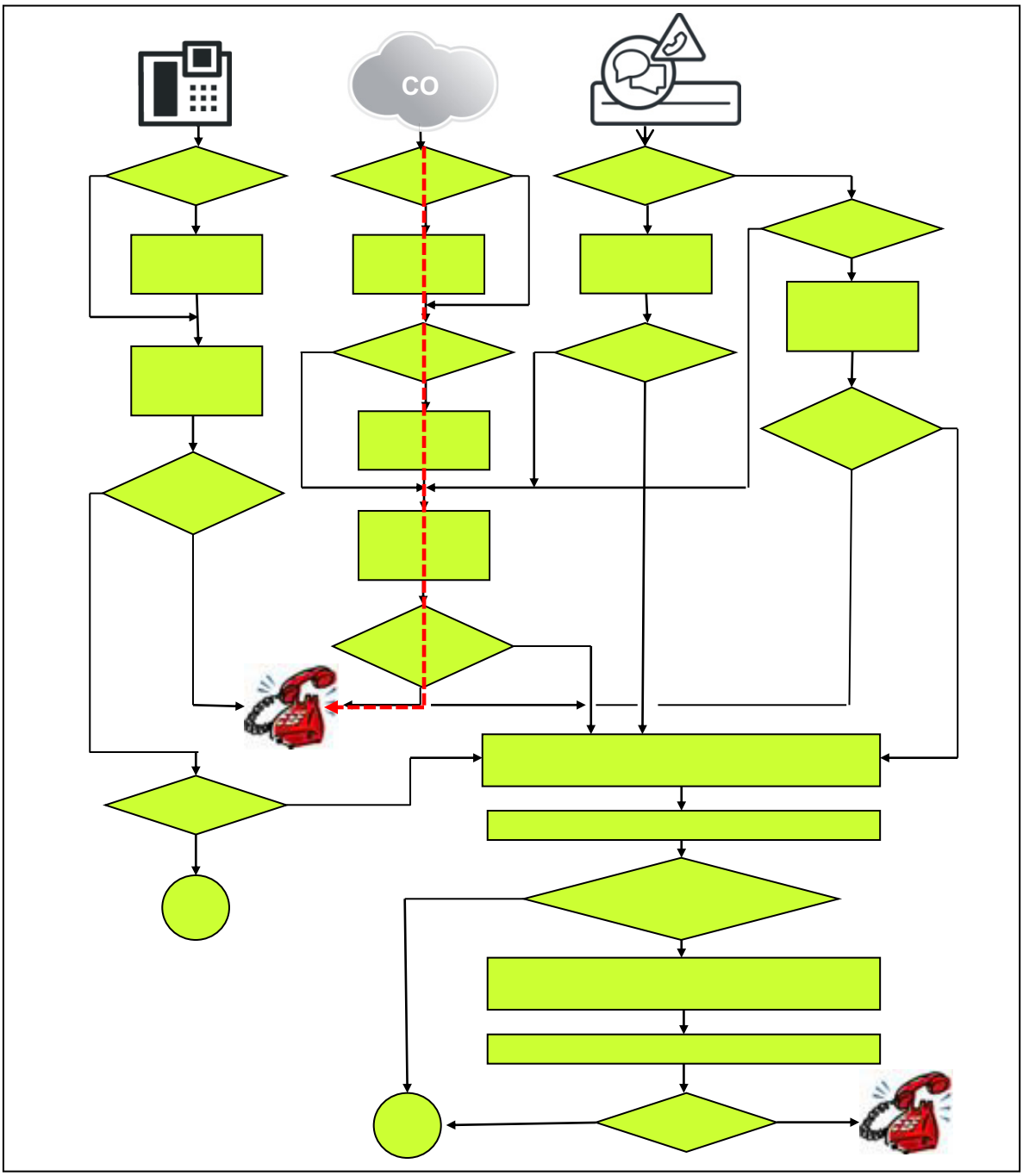
Zusätzlich zu den Daten des vorherigen Szenarios "Teilnehmer A ruft Teilnehmer B über öffentliche Rufnummer" muss im LCR ein geeignetet Wahlplan-Eintrag zur Belegung der Amtsleitung vorhanden sein (z. B. "0CZ").

Die LCR-Wegetabelle und der Wahlplan müssen dem entsprechend eingerichtet sein.



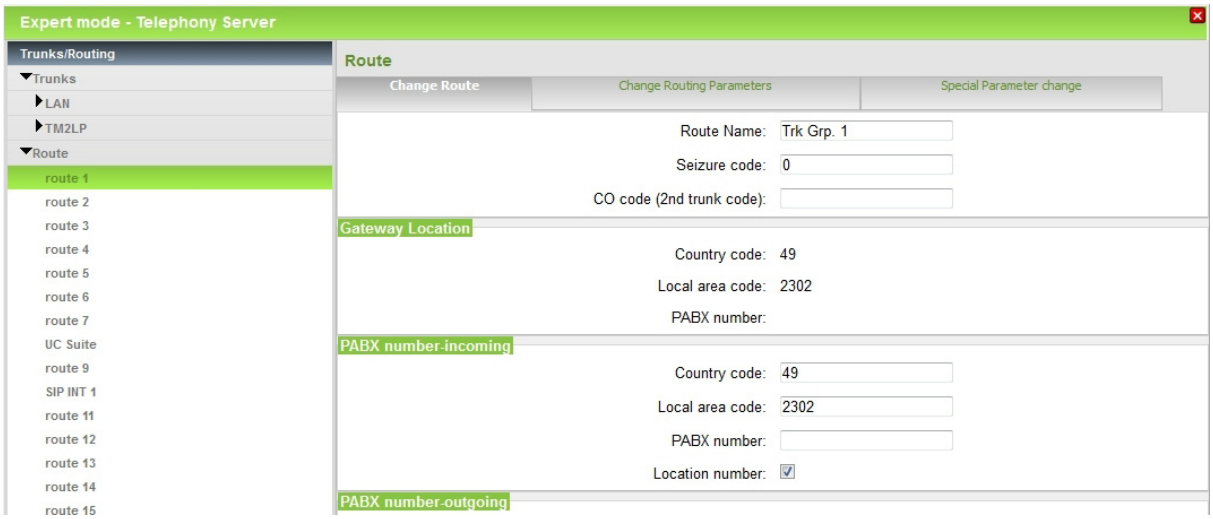
15.3.4.4 ISDN-Amt ruft Teilnehmer A





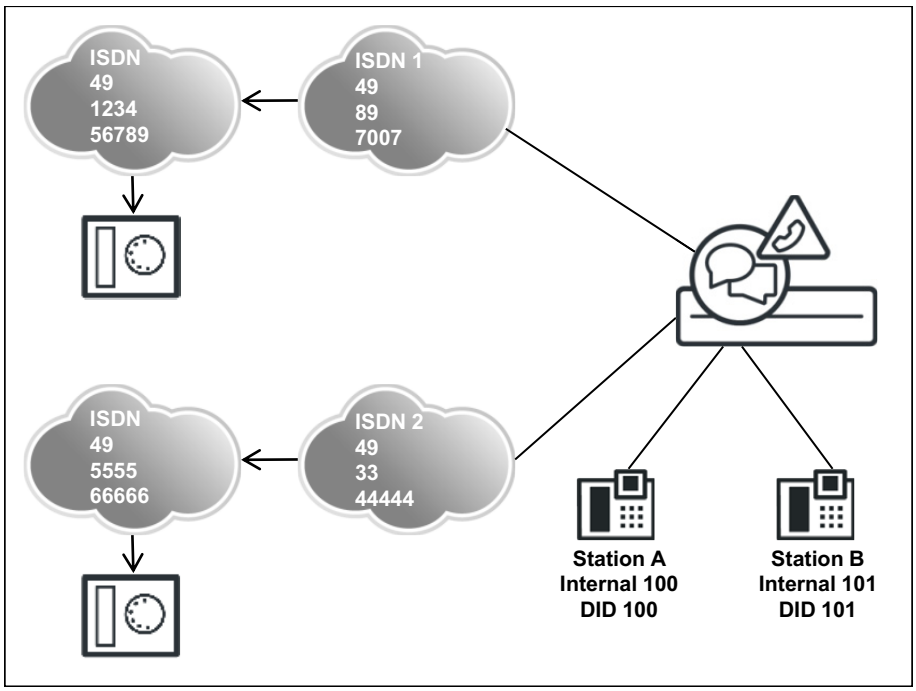
Bei einem kommenden Anruf über ISDN-Trunk wird die Zielrufnummer anhand der Konfigurationsdaten der Anlagenrufnummer kommend (PABX number incoming) der Richtung abgestrippt. Mit dem verbleibenden Rest der Zielrufnummer (Duwa) wird nach einem Ziel im Duwa-Wahlplan gesucht.

Die Parameter des Gateway-Standorts bzw. des Flags **Standort-Nummer** spielen für dieses Szenario keine Rolle.

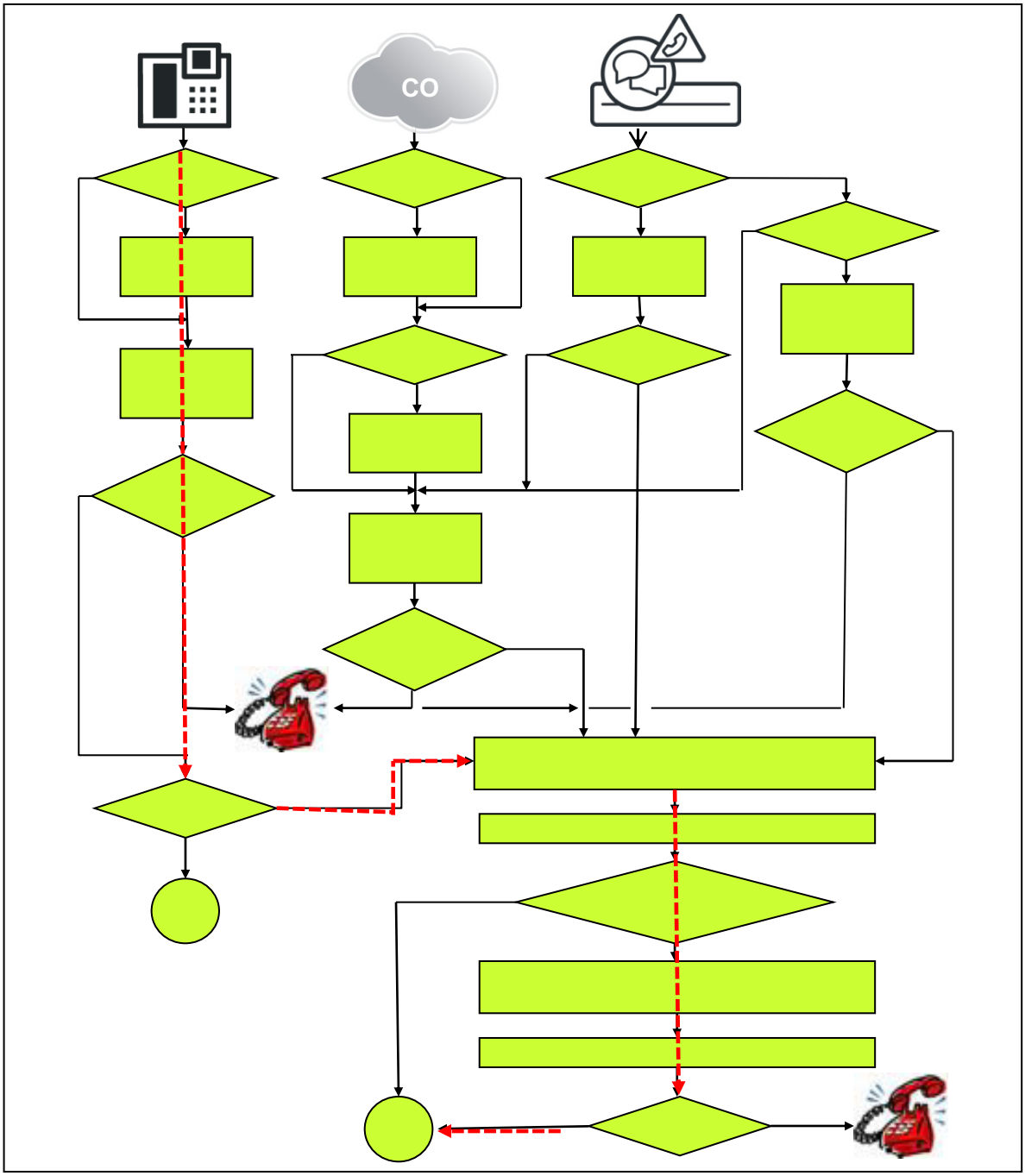


15.3.4.5 Sonderkonfigurationen

Sonderkonfigurationen und entsprechende Auswirkungen: 2 Amtsrichtungen



Teilnehmer A ruft externen Tln über Amtsanschlus 1 bzw. 2



Beispiel:

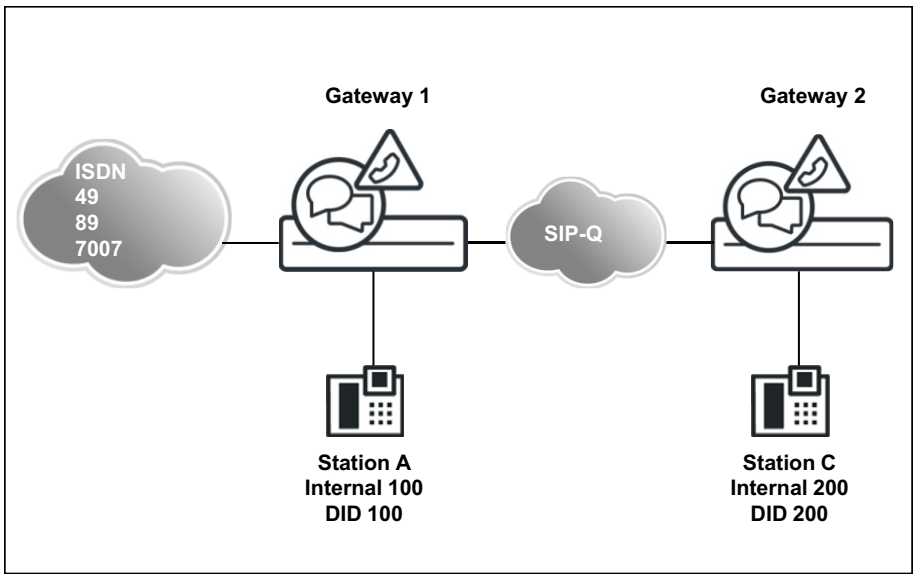
- Ein Kunde möchte einen Standard-Anschluß ISDN 1 verwenden. Dieser wird als Standortnummer eingerichtet.
- Additiv wird ein zweiter Anschluß ISDN 2 für besondere Anwendungen verwendet.

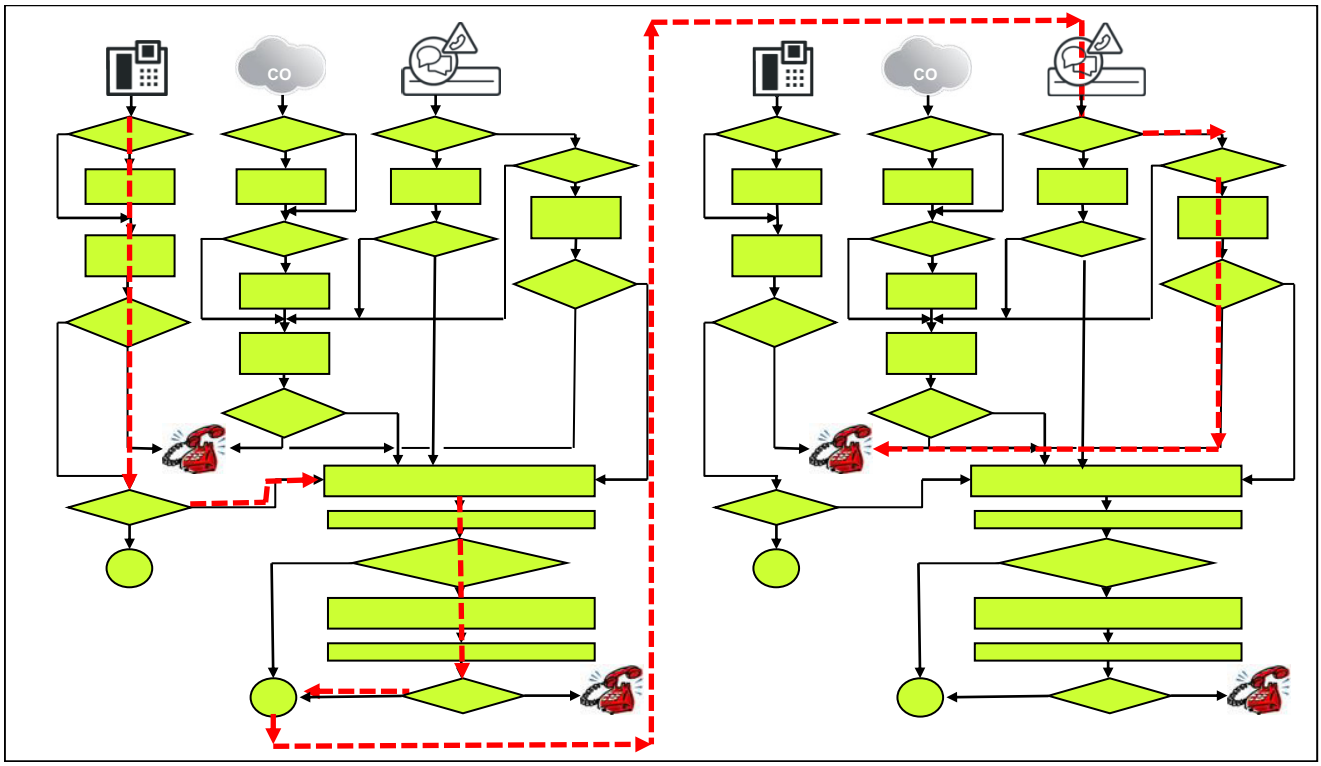
Hinweise bzw. Einschränkungen:

- Nur EINE Amtsrichtung (ISDN 1 = Standort des Systems) wird in vollem Umfang unterstützt, d. h. es kann keine Mehrkundenkonfiguration (Gemeinschaftsanlage) mit gleichberechtigten Amtsanschlüssen eingerichtet werden.
- Der additive Amtsanschluß ISDN 2 kann für Basic Call (kommend/gehend) verwendet werden.
- In komplexen Vermittlungsszenarien kann eine korrekte Rufnummerndarstellung unter Umständen nicht sichergestellt werden.
- Bei Anschaltung von Applikationen wird nur die Standort-Rufnummer unterstützt, ebenso die Wahl von internen Zielen mit öffentlicher Rufnummer.
- Die Konfiguration leitet sich bzgl. Richtungskonfiguration und LCR aus den vorangegangenen Beispielen ab.

15.3.4.6 Teilnehmer A ruft Teilnehmer C über Internrufnummer

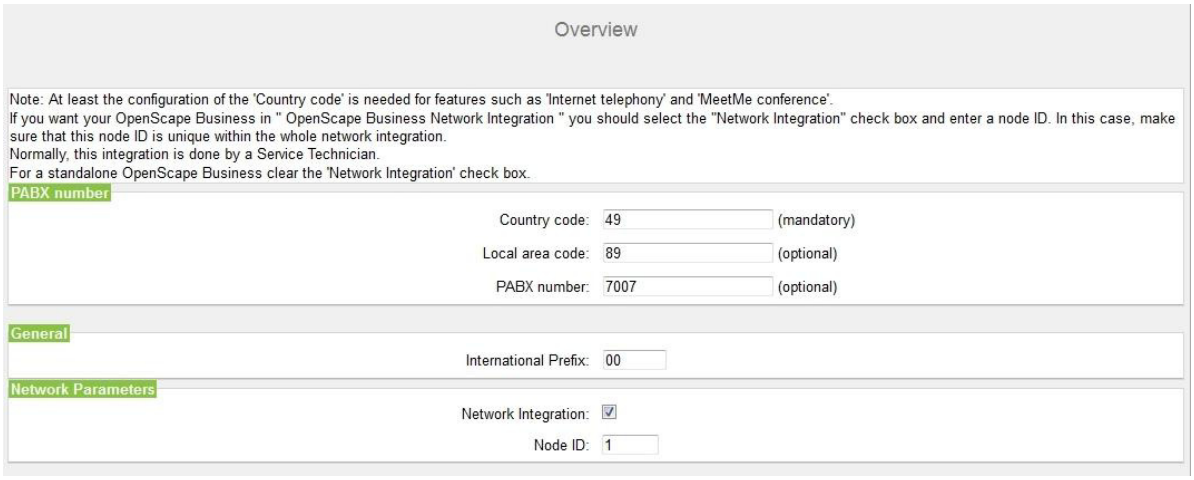
Vernetztes Kommunikationssystem als Unteranlage (ohne Amtsleitung)





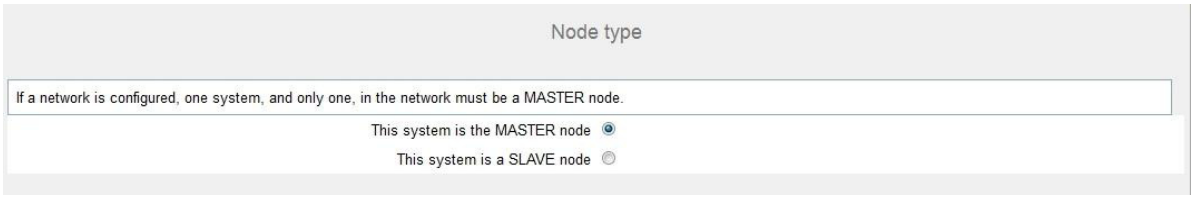
Voraussetzungen der Standalone-Systeme vor der Vernetzung:

- Beide Kommunikationssysteme haben eindeutige IP-Adressen und sind im IP-Netz des Kunden eingebunden.
- Beide Kommunikationssysteme sind per WBM im Kundennetz administrierbar.
- In der Basisinstallation ist je Kommunikationssystem eine eindeutige Knoten-ID für die Vernetzung vergeben (z B. System 1 = Knoten-ID 1 und System 2 = Knoten-ID 2).
- Festlegung der Nummerierung in der Basisinstallation der Systeme 1 und 2: Die Nummerierung der Standalone-Systeme muss die geschlossene Nummerierung im späteren Netzverbund berücksichtigen.
- Dieses Beispiel geht davon aus, dass eine geschlossene Nummerierung (bei Einsatz von UC-Suite zwingend!) zum Einsatz kommt, Konfiguration über Netzwerk-Wizard. Bei einer offenen Nummerierung (möglich bei UC-Smart) wird der Netzwerk-Wizard nicht verwendet. Bei einer Anbindung von OpenScape Voice und OpenScape 4000 ebenfalls nicht.



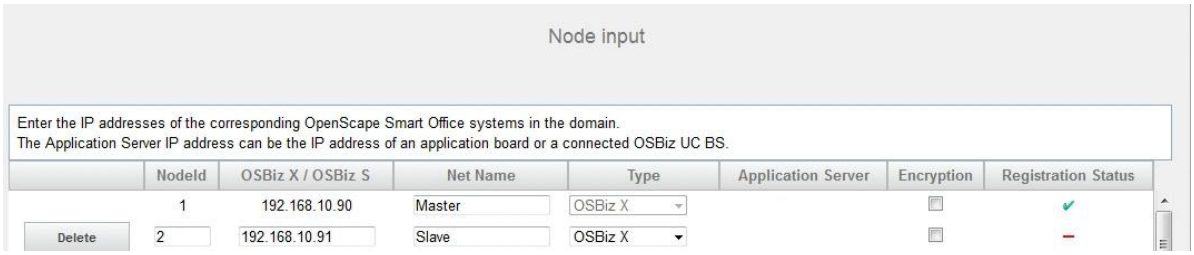
Starten des Netzwerk-Wizard im System 1. Dieses System (dieser Knoten) wird zum Master deklariert). Der Master hat verschiedene zentralen Funktionen im Netzverbund (z. B. Administration, Lizenzverwaltung bei zentraler Lizenzierung, CSP netzweit).

Falls sich eine OpenScape Business S im Netzverbund befindet, sollte diese bevorzugt zum Master erklärt werden (Bandbreite, Performance).



Je Knoten werden die IP-Adressen eingetragen, damit sich die Systeme nach Abschluss der Administration selbstständig finden. Unter **Typ** stehen die OpenScape Business Systeme.

Dieser Dialog ist für Knoten 2 (Slave) ebenfalls durchzuführen.



Bei erfolgreicher Konfiguration synchronisieren beide Systeme (Knoten) ihre Rufnummern und tragen die Rufnummern des anderen Knotens in die CAR-Tabelle ein.

Mit der Erstellung der CAR-Tabellen ist netzweite Telefonie mit Internrufnummern möglich. UC-Suite wird ebenfalls netzweit gestartet. Weitere Schritte zur vollständigen Inbetriebnahme des Netzes stehen in den weiteren Szenarien.

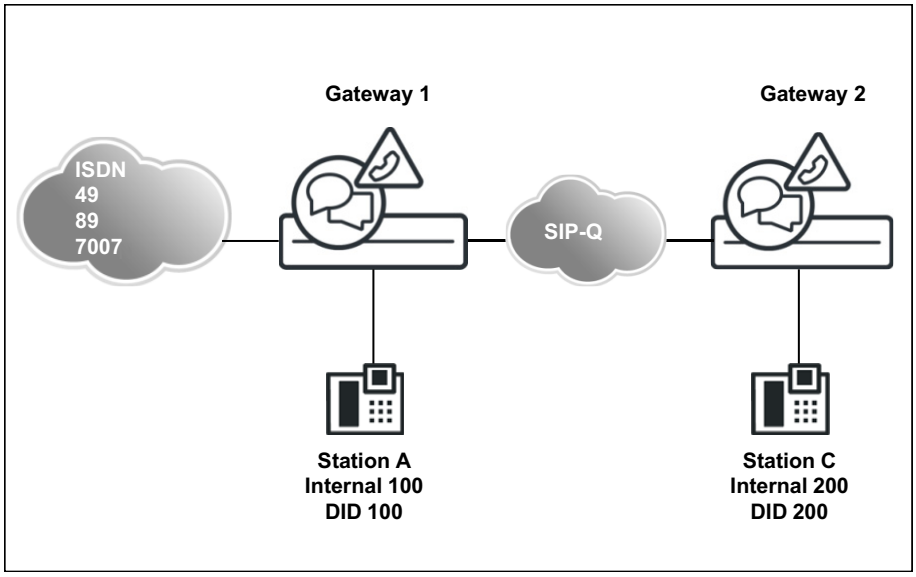
Die Kontrolle der CAR-Einträge ist über **Expertenmodus** > **Sprachgateway** > **Networking** > **Routing** möglich.

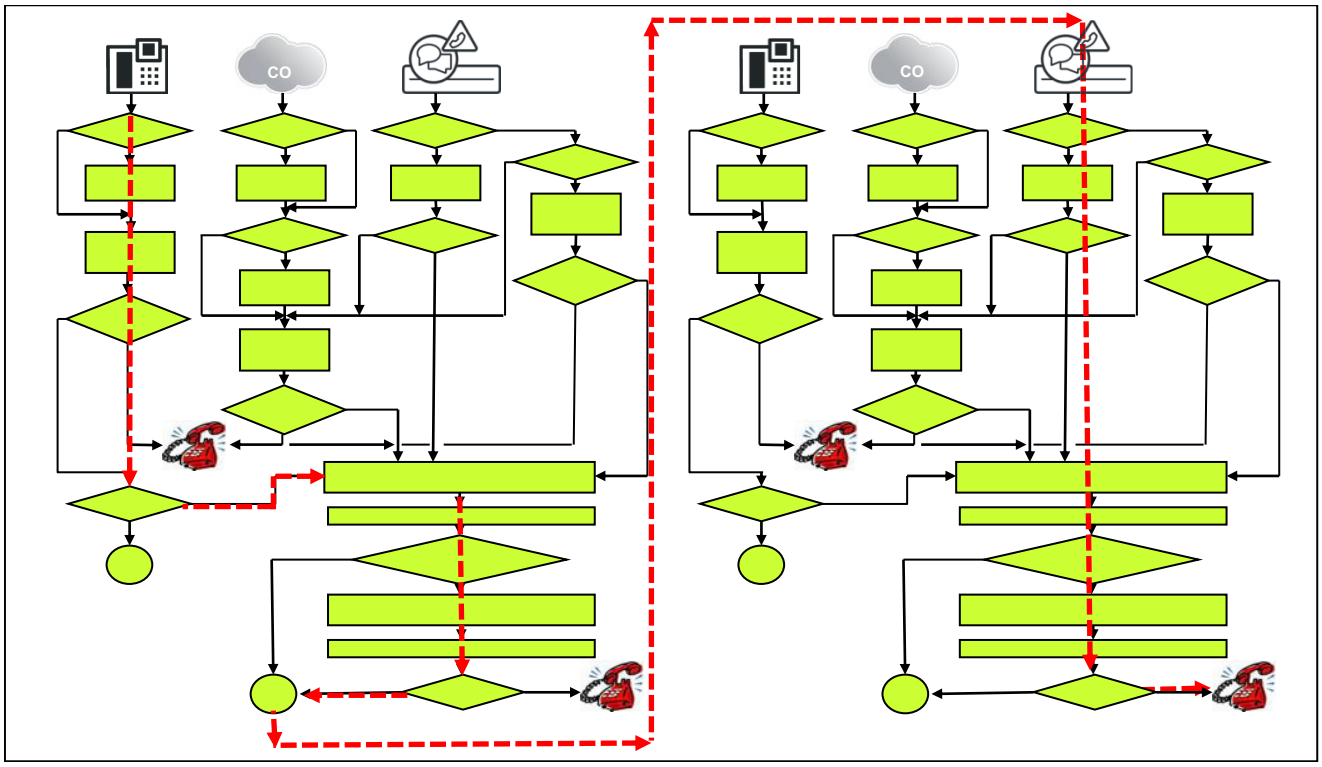
Die Übersicht über die automatische Synchronisierung im Netzverbund sehen Sie im WBM (Sync-Status).

Weitere Netzknoten können jetzt unter dem Menüpunkt **Networking** in der Navigationsleiste im Direktzugriff administriert werden.

15.3.4.7 Teilnehmer A ruft Teilnehmer C über öffentliche Rufnummer im Netzverbund

Vernetztes Kommunikationssystem als Unteranlage





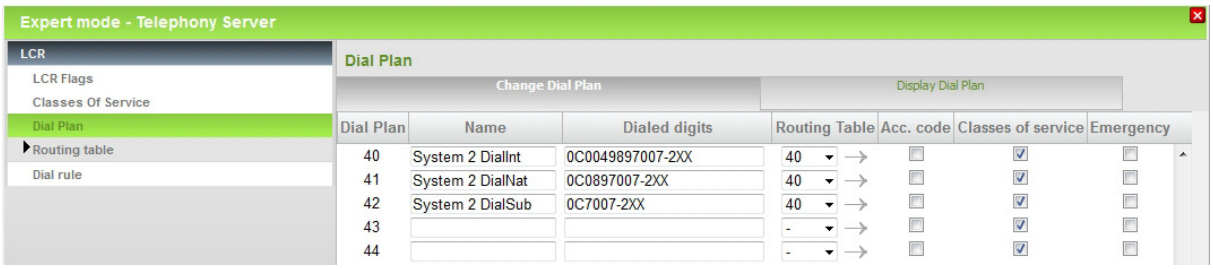
Besonderheiten dieses Szenarios:

- System 1 erkennt, dass die Zielrufnummer nicht zum eigenen System gehört. Die weitere Suche erfolgt daher im LCR. Das Dedizierte Gateway ist im LCR des Systems 1 zur direkten Adressierung der Knoten-ID des Systems 2 zu verwenden. Die Zielrufnummer ist keine Internrufnummer des Netzes (damit wäre sie in der CAR-Tabelle), sondern eine öffentliche Rufnummer, die vom Teilnehmer in drei unterschiedlichen Längen gewählt werden kann:
  Lang = 00049897007nnn
  mittellang = 00897007nnn
  kurz = 07007nnn
  Das Beispiel geht davon aus, dass alle 2xx-Durchwahlnummern Teilnehmer im System 2 sind.

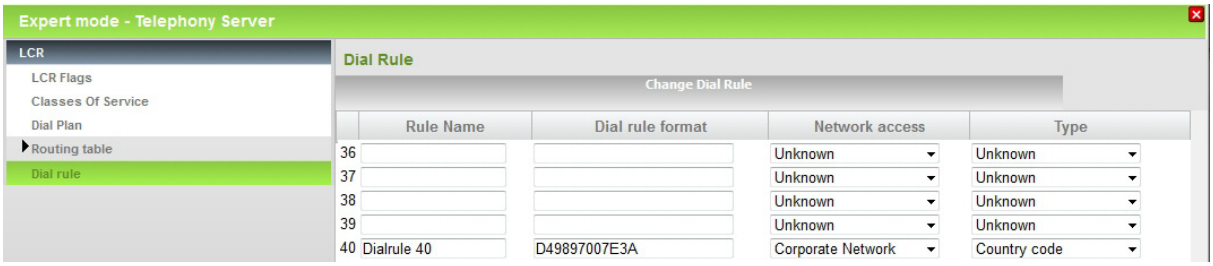
  HINWEIS: Die Wahlplaneinträge müssen so genau konfiguriert werden, dass ALLE getroffenen Rufnummern auch wirklich zum Unterknoten (Netzverbund) gehören. Das kann bei Besonderheiten des Rufnummernplans eine größere Anzahl Einträge erforderlich machen, z. B. bei geteiltem Amtsanschluss oder einer MSN-Konfiguration.

- Im Knoten 2 wird eine Standortnummer mittels "Dummy-Amtsrichtung" mit den Standortdaten von Knoten 1 (Gateway) eingetragen, damit die Zielrufnummer bei der öffentlichen Wahl abgestrippt werden kann, bevor nach einem internen Ziel in Knoten 2 gesucht wird.

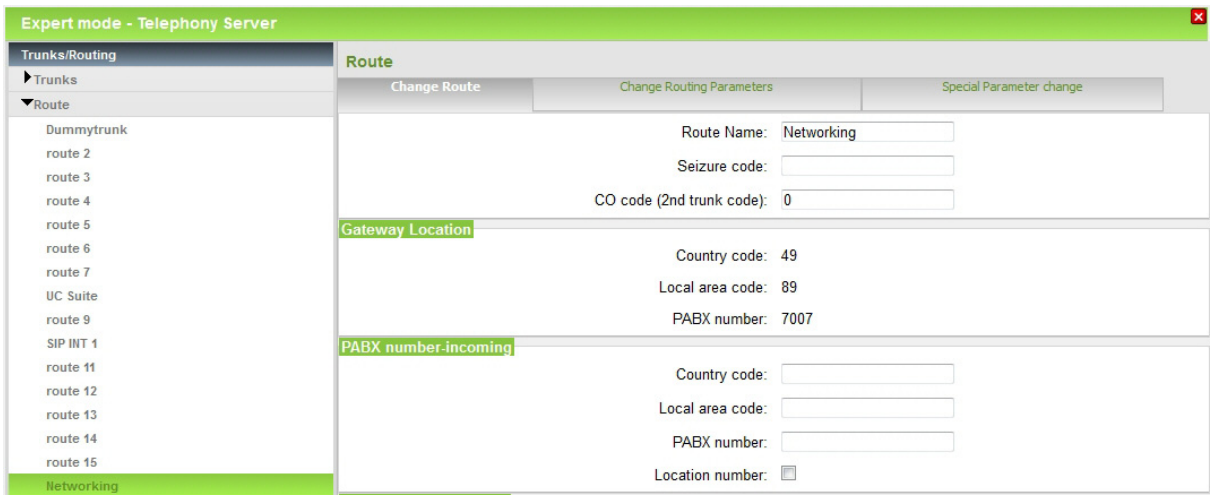
Konfiguration von Knoten 1, Einrichtung im LCR über Dediziertes Gateway





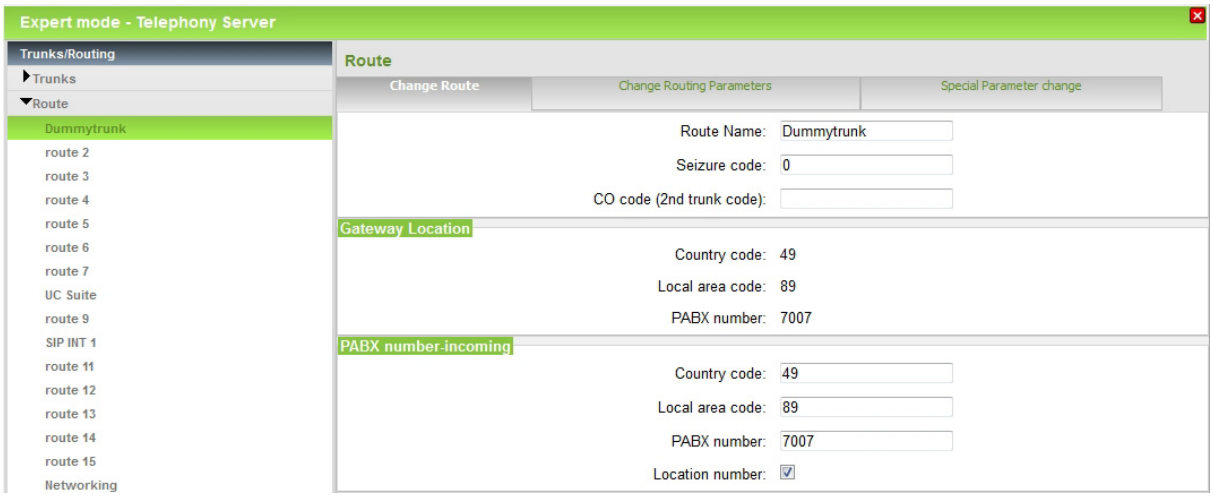


Konfiguration von Knoten 2, Einrichtung der Richtung "Networking"



In der Registerkarte **Routing Parameter ändern** ist die Richtungsart **PABX** einzutragen.

Konfiguration von Knoten 2, Einrichtung der Standortnummer an der "Dummy-Amtsrichtung"



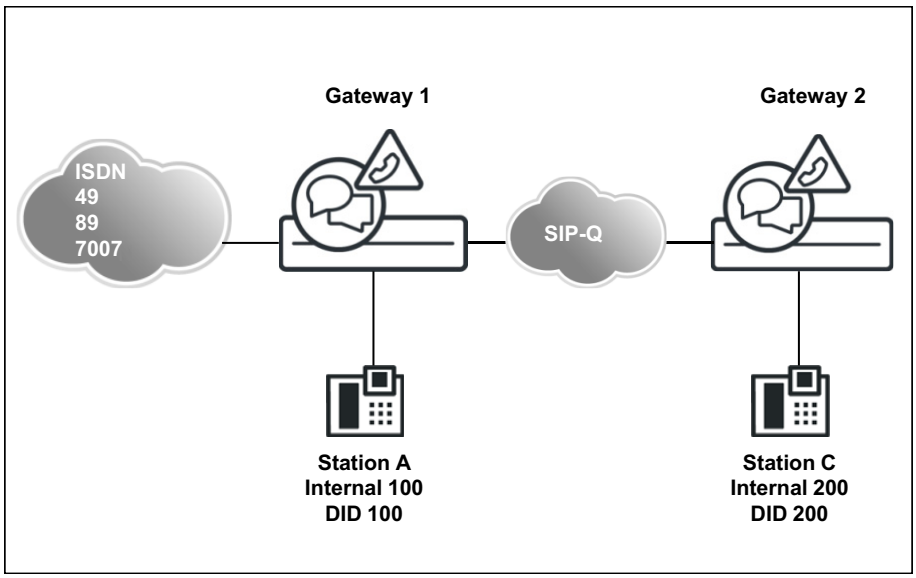
In der Registerkarte **Routing Parameter ändern** ist die Richtungsart **Amt** einzutragen.

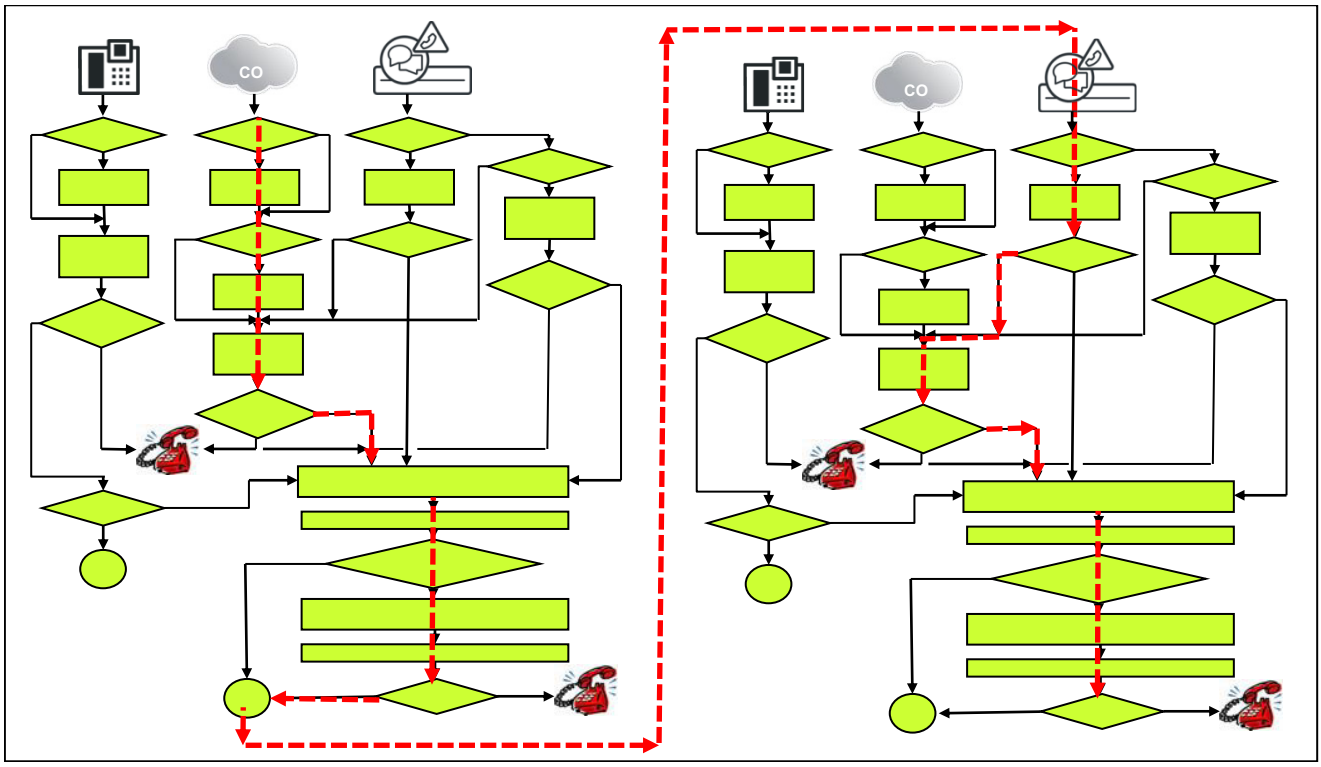
Konfiguration von Knoten 2, Einrichtung im LCR über Dediziertes Gateway

Im Knoten 2 werden alle öffentlichen Rufnummern, die nicht zum eigenen Knoten gehören, zum Knoten 1 geroutet (Standardwahl z. B. 0CZ)

15.3.4.8 ISDN-Amt ruft Teilnehmer C

Vernetztes System als Unteranlage





Beispiel: Kommender Anruf mit Zielrufnummer mit TON = Teilnehmer

Besonderheiten dieser Konfiguration

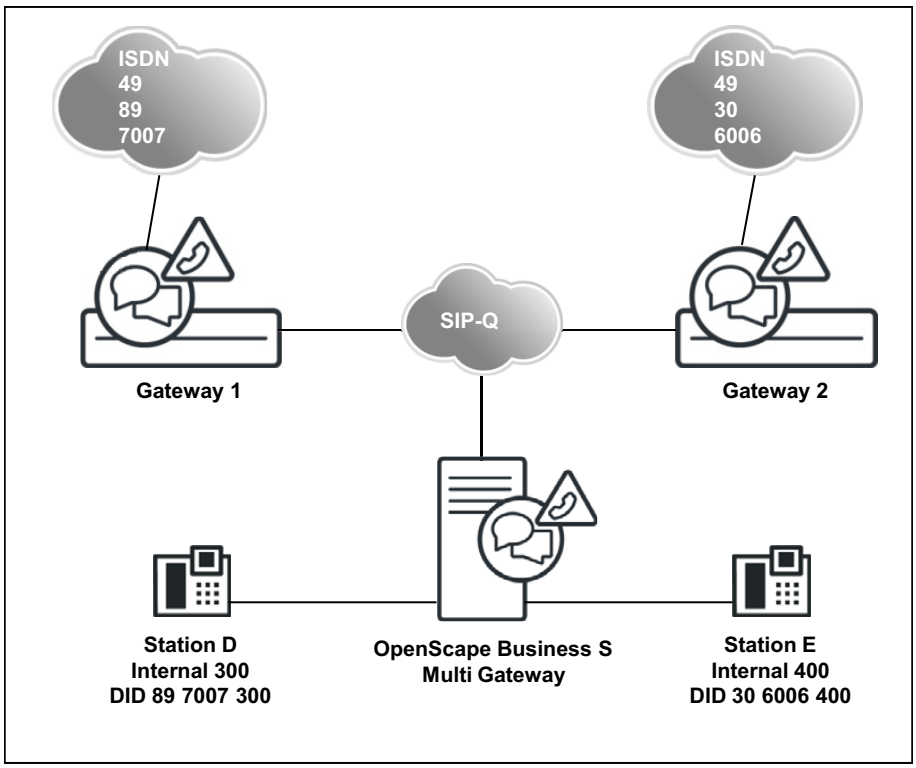
- Knoten 1 ist, wie im vorherigen Szenario beschrieben, einzurichten.
  Die Adressierung von Knoten 2 erfolgt in beiden Fällen mit der öffentlichen Rufnummer, und zwar unabhängig davon, ob der Ursprung der Verbindung in Knoten 1 (Teilnehmer des Systems 1) oder im öffentlichen Netz liegt.

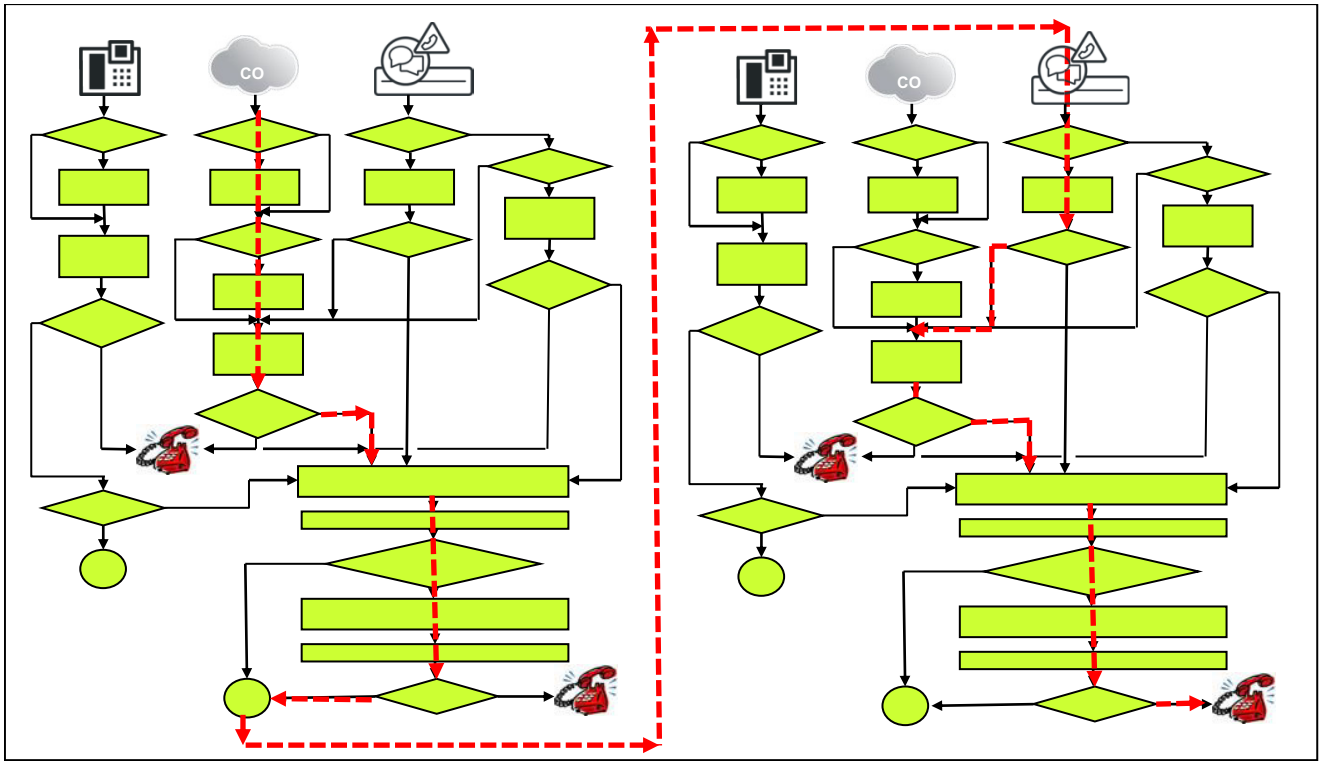
  INFO: Die Wahlplaneinträge müssen so genau konfiguriert werden, dass ALLE getroffenen Rufnummern auch wirklich zum Unterknoten (Netzverbund) gehören. Das kann bei Besonderheiten des Rufnummernplans eine größere Anzahl Einträge erforderlich machen, z. B. bei geteiltem Amtsanschluss oder einer MSN-Konfiguration.

- Knoten 2 ist ebenfalls, wie im vorherigen Szenario beschrieben, einzurichten.

15.3.4.9 ISDN-Amt Gateway 1 ruft Teilnehmer D

Vernetztes System in einer Multi Gateway Konfiguration





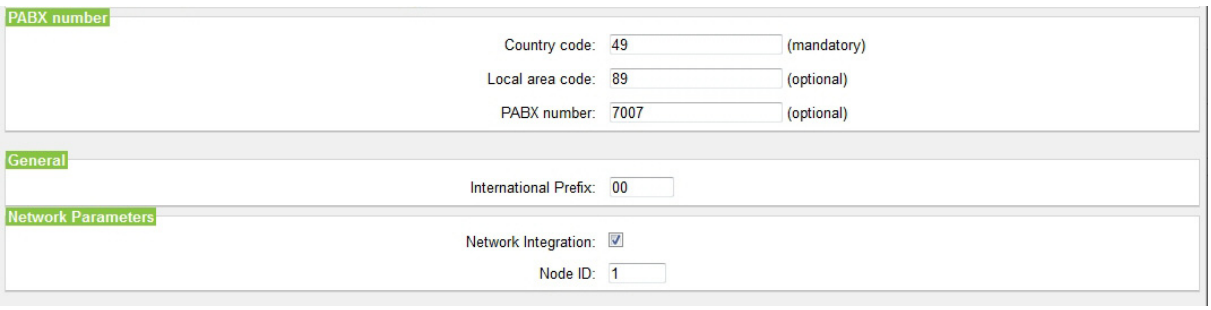
Beispiel: Kommender Anruf mit Zielrufnummer mit TON = Teilnehmer

Konfiguration

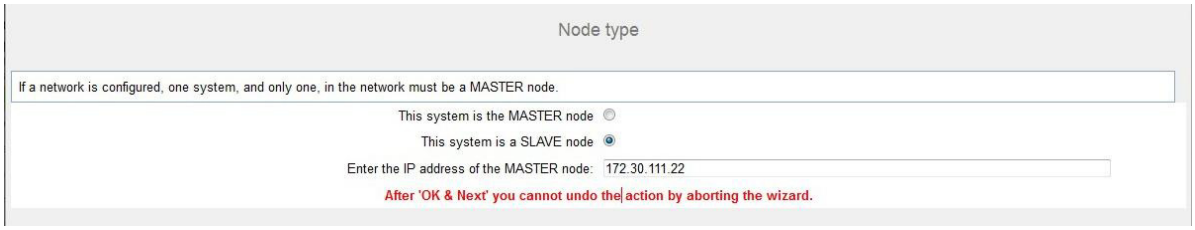
Besonderheiten in diesem Szenario:

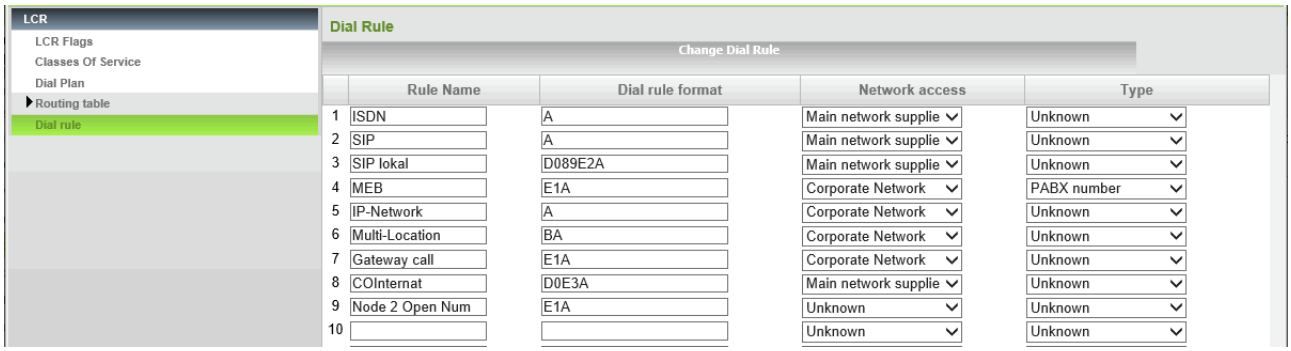
- Das Gateway 1 wird im Prinzip wie im vorherigen Szenario (Gateway 1) eingerichtet, d. h. zunächst Basisinstallation und dann den Netzwerk-Wizard durchlaufen. Wesentlicher Unterschied: Die Gateways werden als Slave, die OpenScape Business S wird als Master eingerichtet (Performance, Bandbreite Lizenzierung).
- In diesem Beispiel werden nur die wesentlichen Unterschiede zum vorherigen Szenario genannt.

Basisinstallation von Gateway 1



Netzwerk-Wizard für Gateway 1





In der OpenScape Business S ist die Zielrufnummer bereits im "National-Format" als DuWa eingetragen.

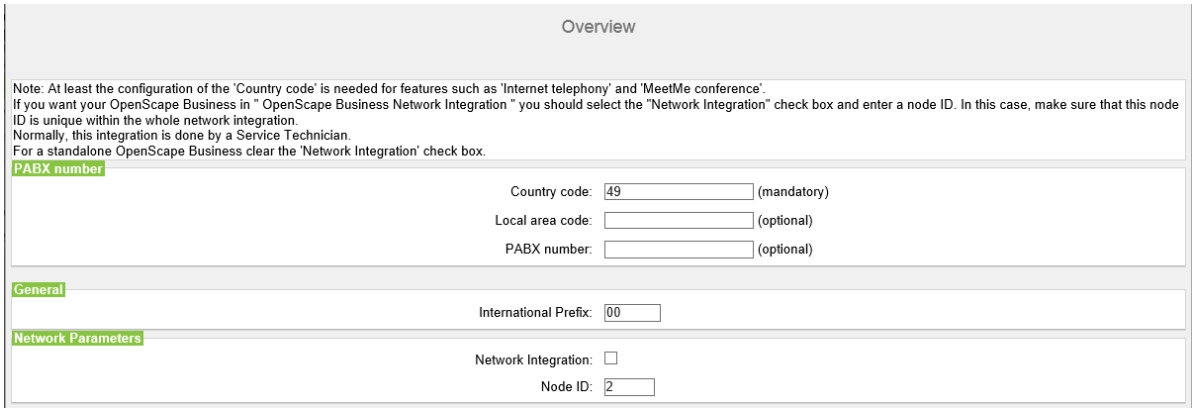
"BA" (Broaden all) hat nur im Gateway eine Bedeutung.

"BA" wird nur benötigt, wenn die ursprüngliche Zielrufnummer TON unknown empfangen wurde, d. h. nur die "kurze DID" = Nebenstellen-Anteil enthält.

Konfiguration des Multi Gateway, OpenScape Business S

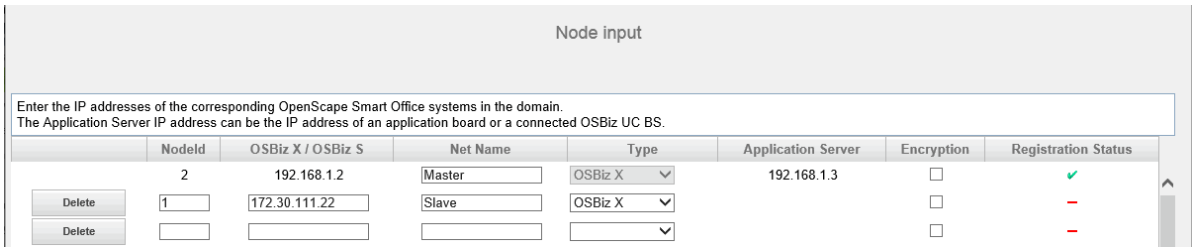
- Erst wird die Basisinstallation, dann der Netzwerk-Wizard durchlaufen.
- Für jeden Teilnehmer der OpenScape Business S werden eingerichtet:
  - Internrufnummer im Kurzformat (z. B. 300)
  - DUWA-Rufnummer im nationalen Format (z. B. 89 7007 300)
  - Zugehörige Gateway Knoten-ID

Basisinstallation der OpenScape Business S, Multi Gateway



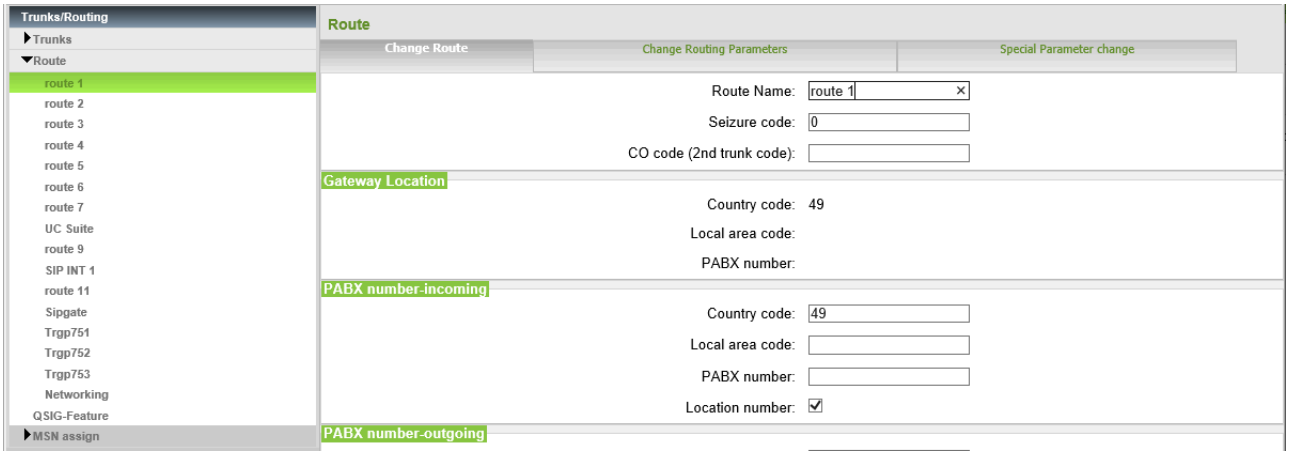
> ***INFO:*** Bei Anlagendaten nur den Country Code eintragen, der Rest der Gesamt-Rufnummer steht im DID-Eintrag der Teilnehmer.

Netzwerk-Wizard der OpenScape Business S, Multi Gateway



Wählen Sie Multi Gateway in der Netzwerk-Konfiguration aus.

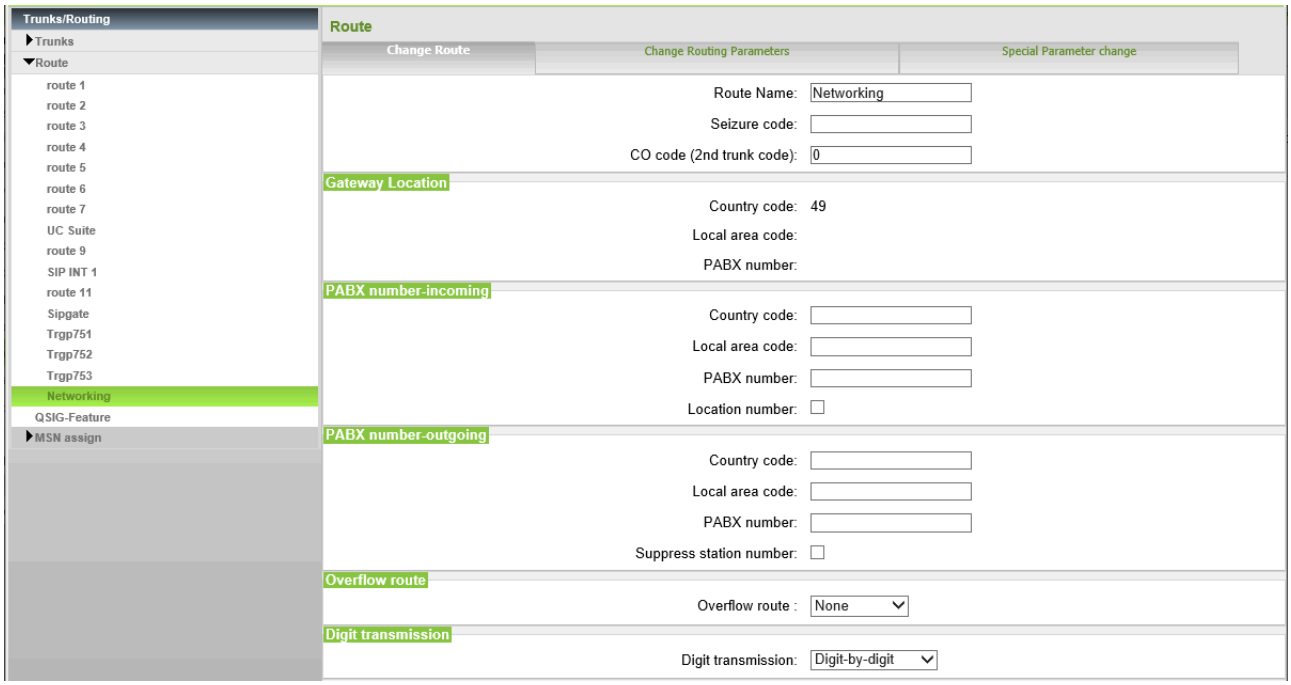
Richtungen der OpenScape Business S, Multi Gateway



Der Country Code wurde bereits im wizard eingetragen.

Routing Parameter: Richtungsart Amt

Diese Richtung bekommt die Richtungsart "Amt".

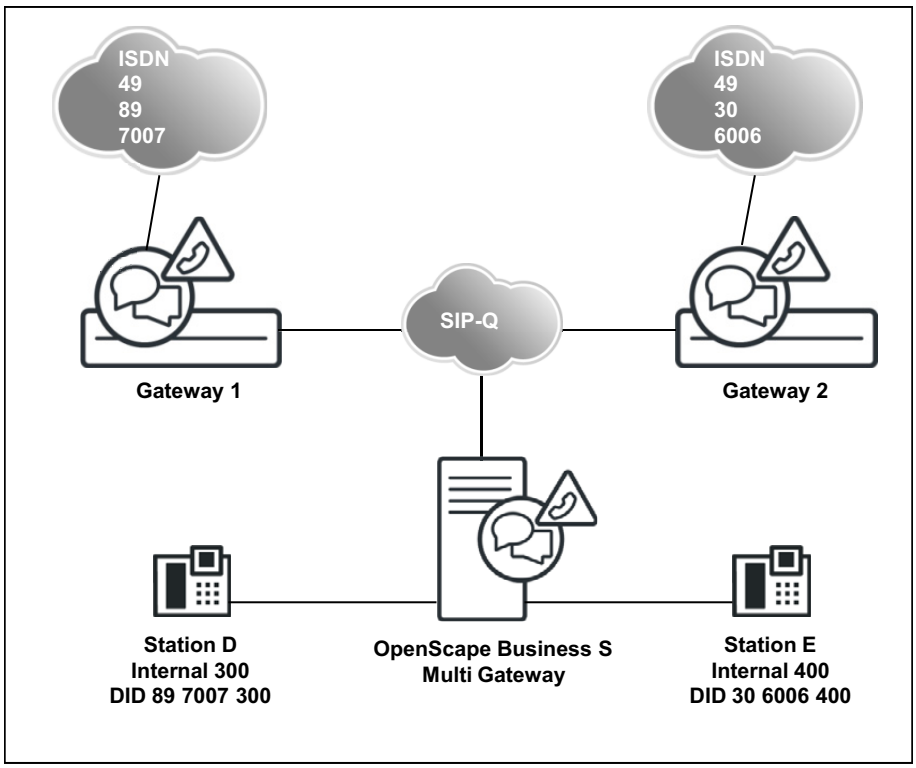


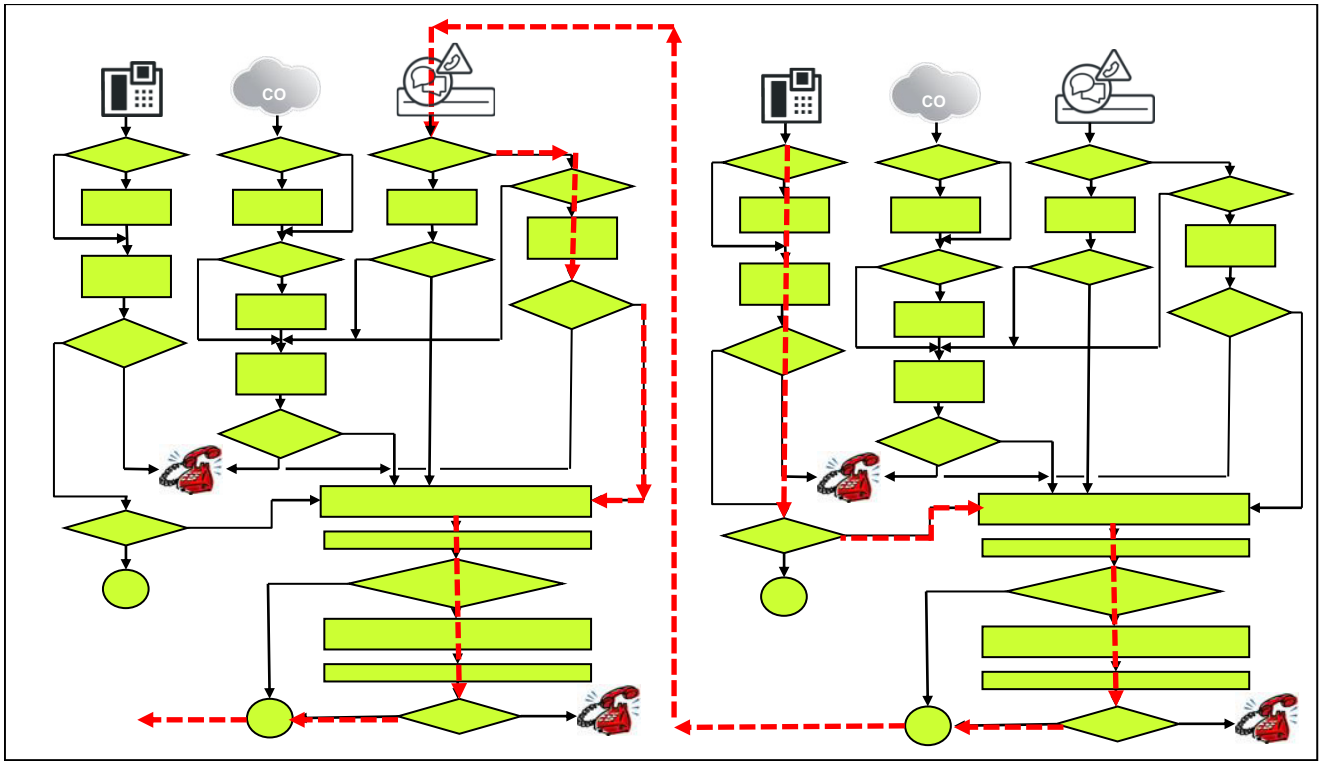
Routing Parameter: Rufnummerntyp outgoing=National, Richtungsart PABX

Diese Richtung bekommt die Richtungsart "PABX" und der NR-Typ gehend ist mit **Ortsnetzkennzahl** einzurichten.

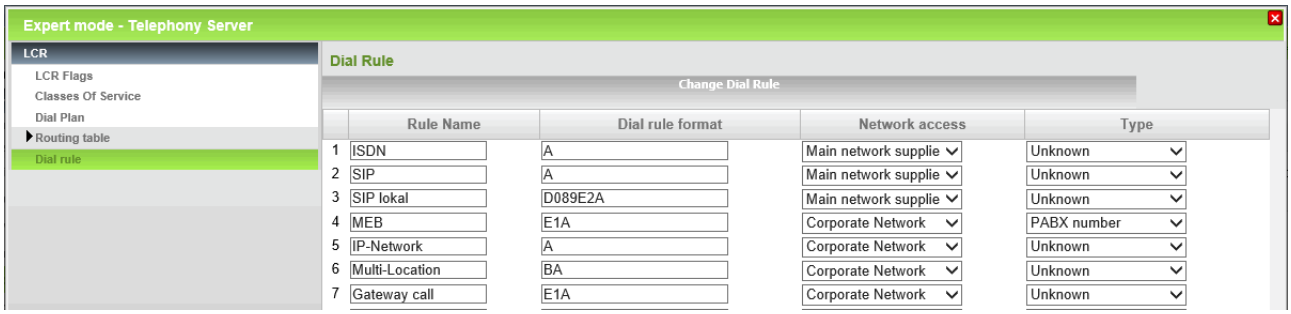
15.3.4.10 Teilnehmer D ruft externen Teilnehmer über Amt

Vernetztes System in Multi Gateway Konfiguration

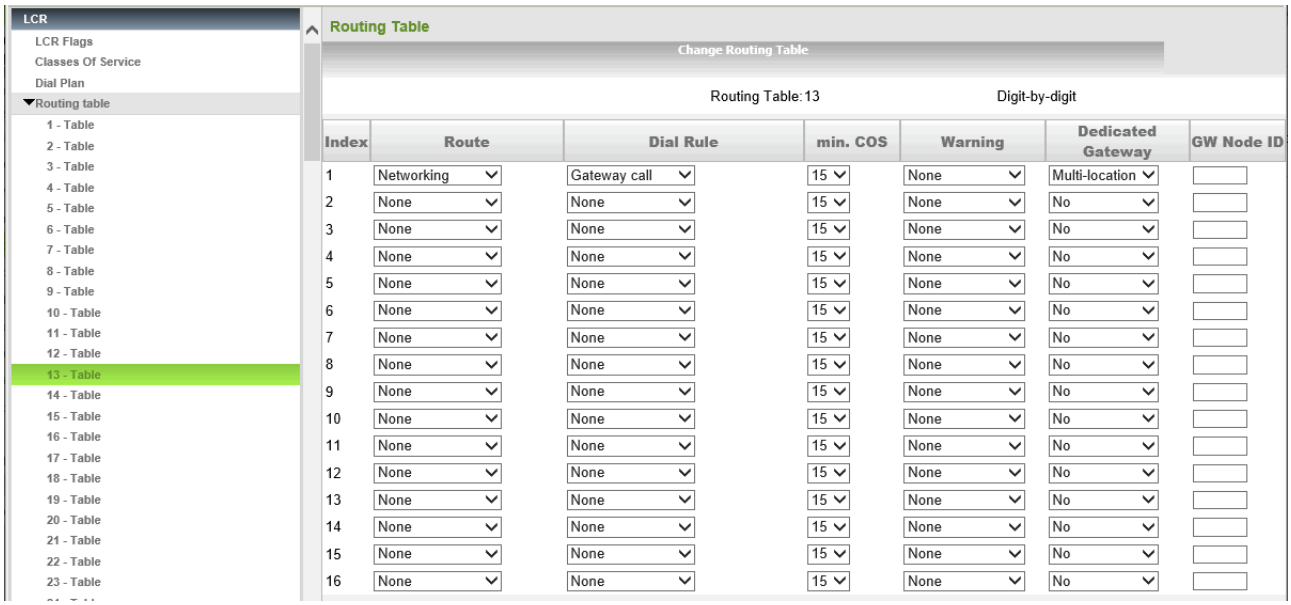

ISDN
49
89
7007
ISDN
49
30
6006
SIP-Q
Gateway 1
Gateway 2
Station D
Internal 300
DID 89 7007 300
OpenScape Business S
Multi Gateway
Station E
Internal 400
DID 30 6006 400


CO
CO

Konfiguration der OpenScape Business S, Multi Gateway



Routing der OpenScape Business S, Multi Gateway, zu den Gateways



Die Einrichtung von Gateway 1 erfolgt wie im vorherigen Beispiel, bei Gateway 2 gilt dies ebenfalls.

15.4 Notrufe

Das Kommunikationssystem und die angeschlossenen Telefone bieten verschiedene Möglichkeiten einen Notruf abzusetzen. Der Administrator kann eine Hotline/Röchelschaltung oder einen Notrufdienst konfigurieren.

Wurde die Activation Period noch nicht gestartet oder befindet sich das Kommunikationssystem in der Failover Period, können Notrufe immer von den beiden ersten aktiven Telefonen abgesetzt werden.

Voraussetzung

Die Notrufzentrale wird durch Wahl der Amtskennziffer (z. B. 0) und der Notrufnummer (z. B. 112) erreicht. Aus Applikationen muss deshalb die Wahl der Zielrufnummer für Notrufe mit führender Amtskennziffer erfolgen.

Prinzipieller Ablauf

Notrufe werden von einem Teilnehmer des Kommunikationssystems durch die Wahl von Amtskennzahl und Notrufnummer initiiert. Die Notrufnummer wird vom Kommunikationssystem an den jeweiligen Provider (PSTN oder ITSP) übergeben.

Fall 1: Wahl des Notrufs über PSTN-Leitung

Der Notruf wird in dem Ortsnetz abgesetzt, dem der Anschluss des Kommunikationssystems zugeordnet ist. Folgendes ist dabei zu beachten: Alle Teilnehmer, die sich nicht am selben Standort des Kommunikationssystems aufhalten, (z. B. Mobility-Teilnehmer, CallMe-Benutzer (Teleworker) oder über WAN abgesetzte Telefone) sollten den Notruf über Handy bzw. ein anderes Festnetztelefon wählen, um den Notruf im Ortsnetz ihres Standortes abzusetzen.

Fall 2: Wahl des Notrufs über ITSP

Nicht alle ITSPs unterstützen Notrufe. In diesem Fall muss per LCR-Konfiguration dafür gesorgt werden, dass Notrufe über PSTN geroutet werden.

Fall 3: Spezielle Vereinbarung mit ITSP oder PSTN-Providern

Für den Fall, dass sich nicht alle Teilnehmer des Kommunikationssystems an einem Standort aufhalten, jedoch fest einem Standort ohne eigenes PSTN zugeordnet sind, kann in Zusammenarbeit mit dem Provider eine individuelle Prozedur zur Notrufsignalisierung festgelegt werden. Z. B. Abhängig von der Anrufer-ID des Rufers kann der Notruf durch den Provider zum entsprechenden vereinbarten Ortsnetz geroutet werden. Diese Vereinbarungen sind individuell und unterliegen keiner Richtlinie.

Fall 4: Notrufe bei Mobile Logon (IP-Mobility)

Mobile Logon (IP-Mobility) bedeutet, dass Teilnehmer das Telefon wechseln und dabei ihre Rufnummer mitnehmen.

Notrufe funktionieren in diesem Fall, solange die Telefone an den Standorten der Gateways angemeldet sind. Alle Teilnehmer, die sich nicht am Standort des Gateways aufhalten, (z.B. Mobility Teilnehmer, CallMe user Homeworker, über WAN abgesetzte Endgeräte) sollten den Notruf über Handy bzw. ein anderes Festnetzendgerät wählen, um den Notruf im Ortsnetz ihres Standortes abzusetzen.

INFO: Für Multigateway-Szenarien, in denen das Leistungsmerkmal Mobile Logon eingesetzt wird, gelten besondere Anforderungen. Die entsprechende Konfiguration wird in Kapitel "Notrufe in Kombination mit Mobile Logon" beschrieben.

15.4.1 Röchelschaltung / Hotline

Für jeden Teilnehmer kann die Hotline-Funktion aktiviert werden. Dabei wird festgelegt, ob beim Abheben des Hörers sofort (Hotline) oder nach einer bestimmten Zeit (Röcheln) die Verbindung zum Hotline-Ziel aufgebaut werden soll.

Röchelschaltung

Wählt der Teilnehmer in der vordefinierten Zeit (Röchelzeit) eine beliebige Ziffer, erfolgt **kein** Verbindungsaufbau zum Hotline-Ziel.

Die Röchelzeit wird vom Administrator zentral konfiguriert und ist individuell für jeden Teilnehmer ein- und ausschaltbar.

Hotline

Bei aktivierter Hotline, hat der Teilnehmer **keine** Möglichkeit, eine Rufnummer einzugeben. Der Teilnehmer kommt immer nach Abheben des Hörers automatisch beim vordefinierten internen oder externen Hotline-Ziel an.

Der Teilnehmer wird immer weitergeleitet, wenn das Hotline-Ziel einer Anrufumleitung oder Rufweiterschaltung folgt.

Systemspezifische Informationen

Der Administrator kann 6 Hotline-Ziele und die Länge der Röchelzeit (0-99 Sekunden) konfigurieren. Gibt der Administrator bei der Röchelzeit den Wert 0 an, wird sofort das Hotline-Ziel gerufen.

Abhängigkeiten

Thema	Abhängigkeit
Anrufschutz	Ist beim Ziel der Anrufschutz aktiviert, hört der Anrufer den Besetztton.

15.4.1.1 Wie Sie einen Hotlineziel konfigurieren und ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Navigieren Sie im Menübaum zu **System > Abwurf/VPL/Hotline**.

4) Unter **Hotline** können Sie 6 verschiedene Ziele (**Ziel-Ruf-Nr.**)eintragen.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

15.4.1.2 Wie Sie die Röchelzeit ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellung**.

3) Klicken Sie im Menübaum auf **System**.

4) Klicken Sie auf **Abwurf/VPL/Hotline**.

5) Unter Hotline können Sie die **Röchelzeit** (Verzögerungszeit in Sekunden,) ändern.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

15.4.1.3 Wie Sie Röcheln oder Hotline für einen Teilnehmer konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Teilnehmer**.

3) Klicken Sie im Menübaum auf **Teilnehmer**.

4) Klicken Sie z. B. auf **IP Clients**.

5) Klicken Sie z. B. auf **System Clients**.

6) Markieren Sie den entsprechenden Teilnehmer und stellen Sie im Feld **Hotline** Modus **Röcheln** oder **Hotline** ein.

7) Haben Sie Hotline eingestellt, dann müssen Sie im Feld Hotline noch die **Anzahl der Hotline-Ziele** einstellen.

8) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

15.4.2 Leitungstrennung für einen Notruf

Wird ein Notruf abgesetzt und es ist keine freie Amtsleitung vorhanden, so wird eine Zwangstrennung ausgelöst. Dem notrufenden Teilnehmer wird automatisch die freie Leitung zugewiesen.

Die Leitungstrennung funktioniert nur bei ISDN-Amtsanschlüssen.

Der Teilnehmer hat die Möglichkeit, bei besetzten Leitungen eine automatische oder manuelle Leitungstrennung durchzuführen.

- Automatisch: Das Leistungsmerkmal Leitweglenkung (LCR) ist aktiv und es ist eine Notrufnummer im LCR hinterlegt.
- Manuell: Das Leistungsmerkmal "Leitung freischalten" ist für den Vermittlungsplatz immer aktiv und wird über Taste oder Kennzahl ausgeführt.

Systemspezifische Informationen

Der Administrator kann beliebig viele Notrufnummern konfigurieren.

Damit eine automatische Leitungstrennung erfolgt, wenn alle Leitungen belegt sind, muss die Notrufnummer im Wahlplan des LCR hinterlegt sein und das Notruf Flag *Experten Mode* für diese gesetzt sein.

15.4.2.1 Wie Sie die Leitungstrennung für einen Notruf aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Routing**.

3) Navigieren Sie im Menübaum zu **LCR > Wahlplan**.

4) Wählen Sie im Fenster **Wahlplan ändern** eine der folgenden Möglichkeiten:

- Wenn Sie die Funktion aktivieren möchten, aktivieren Sie das Kontrollkästchen **Notrufnummer** für die entsprechende Rufnummer.
- Wenn Sie die Funktion deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Notrufnummer** für die entsprechende Rufnummer.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

15.4.3 Nur für USA, Kanada: Notrufdienst E911

Durch den erweiterten Notrufdienst E911 werden neben der Rufnummer auch Informationen über den geographischen Standort (hinterlegte Adresse) des Anrufers beim Absetzen eines Notrufs übermittelt.

Die den Notruf entgegennehmende Rettungsleitstelle ist nicht auf die mündliche Übermittlung des Standortes durch den Anrufer angewiesen.

In den USA greift das Leistungsmerkmal nur dann, wenn die Notrufnummer 911 gewählt wird.

Für den Notrufdienst E911 muss jedem Teilnehmeranschluss mit gültiger Durchwahlnummer eine LIN (Location Identification Number) vom Administrator zugeordnet werden. Räumlich nah zusammen liegende Teilnehmeranschlüsse sind mit der gleichen LIN zu versehen. Eine Datenbasis in der Notrufzentrale, in der alle LIN gespeichert sind, identifiziert anhand der übermittelten LIN den Namen und die Adresse des Notrufenden.

Abhängigkeiten

Thema	Abhängigkeit
CLIP	Für USA ist standardmäßig LIN aktiviert. Wenn allerdings CLIP (Calling Line Identification Presentation) für USA aktiviert wird, so ist automatisch LIN deaktiviert.

15.4.3.1 Wie Sie CLIP / LIN bearbeiten

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Teilnehmer**.

3) Klicken Sie im Menübaum auf **Teilnehmer**.

4) Klicken Sie z. B. auf **IP Clients**.

5) Klicken Sie auf die Registerkarte **Teilnehmer ändern**.

6) Tragen Sie beim entsprechenden Teilnehmer im Feld **CLIP/LIN** die 16-stellige LIN ein.

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

15.4.4 Notrufe in Kombination mit Mobile Logon

Wenn man das Leistungsmerkmal Mobile Logon in einem Multi-Gateway-Netzverbund verwendet, kann bei einem Wechsel des Telefons auch der physikalische Standort wechseln. Daher sind besondere Maßnahmen für das Routing von Notrufen erforderlich.

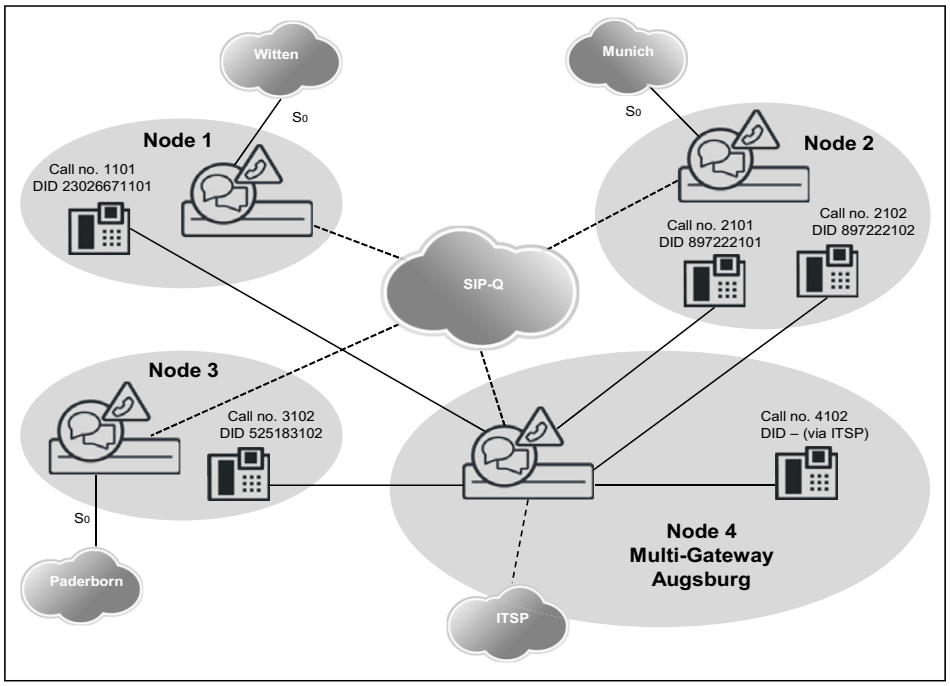
Algorithmus-Beschreibung für die Wahl eines Notrufs

Wenn ein Teilnehmer eine Notrufnummer wählt (Kennung im LCR), überprüft ein Algorithmus, ob für das Telefon eine Notrufnummer konfiguriert wurde. Diese wird dann zur Erzeugung einer abgeleiteten Rufnummer verwendet, die im Netzverbund zum Routen des Anrufs über das richtige Gateway genutzt wird.

Jede Nummer, die im Wahlplan als Notrufnummer gekennzeichnet ist, hat auch einen Verweis auf einen Eintrag in der Wegetabelle. Jeder Eintrag in der Wegetabelle, der zu einer Notrufnummer gehört, muss mit einer geringen Berechtigungsklasse (COS) versehen sein. Geringe Berechtigungsklasse bedeutet, dass jeder Teilnehmer berechtigt ist eine Notrufnummer abzusetzen.

15.4.4.1 Konfiguration des Notrufszenarios

Die Konfiguration des Notrufszenarios zeigt für einen Multi-Gateway-Netzverbund, welche Schritte für die Einrichtung durchzuführen sind.



Mobile Logon wird nur innerhalb eines Knotens unterstützt, d. h. Standortwechsel - und damit besondere Anforderungen für Notrufe - sind nur für Telefone relevant, die am Multi-Gateway Knoten (4) betrieben werden. Generell sind alle betroffenen Telefone an Knoten 4 angemeldet, befinden sich physikalisch jedoch an verschiedenen Standorten.

- In allen betroffenen Telefonen ist ein Eintrag für Notruf erforderlich (Anschlussanteil der kanonischen Rufnummer des Standort-Knotens + Belegungskennzahl Notruf-Richtung)
- Der LCR-Eintrag (Knoten_4lokal) in der nachfolgenden Tabelle ist nur erforderlich, wenn am Knoten 4 (Multi-Gateway) Telefone physikalisch vorhanden sind.Es wird ebenfalls die Standort-Nummer vorangestellt, die hier aber unvollständig ist (nur Landeskennzahl). Die Voraussetzung dafür ist ein ITSP-Zugang an Knoten 4, der Notrufe ins Ortsnetz unterstützt.

Behandlung von Notrufnummern

- Bei der Wahl am Telefon wird eine mit Notruf gekennzeichnete LCR-Regel (z. B. 0C11x) getroffen.

- Die im Telefon gespeicherte (und bei der Anmeldung ins System übertragene) Notrufnummer wird mit den Standortdaten des Systems (Ländervorwahl, Ortsnetzkennzahl, Anlagenrufnummer) verglichen. Falls unterschiedlich wird eine "lange" Notrufnummer gebildet:
  - Entfernen des Access-Codes: 0112 -> 112
  - Einfügen von <LDAP-Belegungskennzahl><Internationales-Präfix><programmierte Notfallrufnummer>: z. B. 112 -> 0 00 49897220 112
- Die "lange" Notrufnummer wird durch das LCR geroutet, durch spezifische LCR-Regeln entweder direkt ins lokale Amt oder per Querleitung zum jeweiligen Partnerknoten und von dort ins Amt.

> ***INFO:*** Weil im Telefon nicht genau die vollständige Standort-Nummer des lokalen Knotens eingetragen wird, muss auch für den lokalen Notruf am Multi-Gateway-Standort eine geeignete LCR-Regel eingetragen werden.

Einrichtung der Standortdaten für Knoten 4

Knoten 4	Gateway-Knoten
G.-Standort Land	49
G.-Standort Ortsnetz	
G.-Standort Anlage	
Internationales Präfix	00
Nationales Präfix	0
LDAP-Belegungskennzahl	0

Richtungsparameter

Richtung	Nr-Typ gehend	RNR-Typ
Networking	National	Int/Duwa

Richtung Networking	
Amtskennziffer (2. AKZ)	0

Knoten 4, Telefone

Standort Witten	
Call Number (Rufnummer)	1101
Emergency Number (Notrufnummer)	4923026670

Standort München	
Call Number (Rufnummer)	2101
Emergency Number (Notrufnummer)	49897220

Standort Paderborn	
Call Number (Rufnummer)	3102
Emergency Number (Notrufnummer)	49525180

Standort Augsburg	
Call Number (Rufnummer)	4102
Emergency Number (Notrufnummer)	490

Übersicht der für einen Notruf relevanten Einträge im LCR für Knoten 4

Wahlplan			Wegetabelle			Wahlregel		
Name	**Gewählte Ziffern**	**Not-betrieb**	**Richtung**	**Dedizier-tes Gate-way**	**Gate-way ID**	**Wahlregel**	**Verfahren**	**Typ**
Notruf [1)]	0C112	X	Networking	Multi Gate-way	1	E1A	Corp. Net-work	Unbekannt
Notruf [1)]	0C0110	X						
Amt.	0CZ							
Notruf_nach1	0C00492302667-0-11X	X	Networking	Erzwungen	1	E3A	Corp. Net-work	Unbekannt
Notruf_nach2	0C004989722-0-11X	X			2			
Notruf_nach3	0C004952518-0-11X	X			3			
Notruf_4lokal [2)]	0C0049-0-11X	X	ITSP	Nein		E4A	Hauptnetz-anbieter	Unbekannt

[1)] Mit den obigen Regeln wird in diesem Beispiel nur die Notrufsituation erkannt, aber nicht geroutet. Für das Notruf-Routing wird die abgeleitete "lange" Notruf-nummer verwendet.

[2)] Weil am Multi-Gateway-Standort Teilnehmer physikalisch angeschlossen sind, ist eine eigene LCR-Regel für einen lokalen Notrufzugang einzutragen (via ITSP-Richtung).

15.5 Anrufsteuerungsdienst (Call Admission Control)

Über das Leistungsmerkmal Anrufsteuerungsdienst (Call Admission Control CAC) kann die benutzte Bandbreite über die Anzahl von Gesprächen einge-schränkt werden.

Das Kommunikationssystem bietet drei Möglichkeiten Einfluß auf die benötigte Bandbreite zu nehmen:

- Einschränkung der Anzahl der gleichzeitigen Gespräche über ITSP
- Einschränkung des Bandbreitenbedarfs bei Gateway-Gesprächen
- Einschränkung der Anzahl der Gespräche in Vernetzungsszenarien

15.5.1 Einschränkung der Anzahl gleichzeitiger Gespräche über ITSP

Durch die Konfiguration der verfügbaren Upload-Bandbreite wird die maximale Anzahl der Anrufe zum ITSP festgelegt. Durch Herabsetzen der Anzahl der Gespräche kann der Bandbreitenbedarf weiter reduziert werden.

Die Einstellungen dazu können in den Wizards **Netzwerk/Internet** und **Zentrale Telefonie** vorgenommen werden.

Die Anzahl der möglichen Anrufe über ITSP kann im **Experten-Modus** unter **Telefonie** > **Sprachgateway** > **SIP-Parameter** eingesehen werden.

15.5.2 Einschränkung des Bandbreitenbedarfs bei Gateway-Gesprächen

Durch Konfiguration der zulässigen Codecs bei Gateway-Gesprächen kann die Bandbreite beeinflußt werden.

Werden nur komprimierende Codecs eingestellt, so ist der Bandbreitenbedarf geringer. Wenn gemischte Codecs genutzt werden, kann die Priorisierung der nicht komprimierenden Codecs herabgesetzt werden, sodass diese seltener verwendet werden.

Die entsprechenden Einstellungen dazu werden im **Experten-Modus** unter **Telefonie** > **Sprachgateway** > **Codec-Parameter ändern** gemacht.

15.5.3 Einschränkung der Anzahl der Gespräche in Vernetzungszenarien

Das Kommunikationssystem bietet zwei Möglichkeiten die Bandbreite in Vernetzungsszenarien zu kontrollieren.

Beschränkung durch die Anzahl der Leitungen zu anderen Netzknoten

Durch Zuordnung einer bestimmten Anzahl von Leitungen zu anderen Netzknoten kann eine Obergrenze aller gleichzeitig möglichen Gespräche von und zu diesen Knoten vorgenommen werden.

Beschränkung der Bandbreite durch gezielte Codec-Auswahl

Die verfügbare Bandbreite kann durch Konfiguration der verwendeten Codecs vom und zum Partner (Ziel-IP-Adresse) festgelegt werden.

Die entsprechenden Einstellungen dazu werden im **Experten-Modus** unter **Telefonie** > **Sprachgateway** > **Ziel-Codec-Parameter hinzufügen** gemacht.

15.6 Gemeinschaftsanlage

Die gesamte Kapazität des Kommunikationssystems kann organisatorisch in maximal sechs Unteranlagen aufgeteilt werden. Dadurch können z. B. mehrere Firmen ein Kommunikationssystem gemeinsam nutzen.

Das Leistungsmerkmal Gemeinschaftsanlage wird durch Ausnutzung vorhandener Leistungsmerkmale realisiert. Das bedeutet, dass keine explizite Einrichtung von Teilanlagen erfolgt.

Die Steuerung von erlaubten und verbotenen Verbindungen zwischen einzelnen Teilnehmern und Leitungen geschieht über die Verkehrsbeziehungsgruppen.

Leistungsmerkmale in der Gemeinschaftsanlage:

- Abwurf
- Anlagenrufnummer
- Anruferliste
- Aufschalten
- DISA
- Direktansprechen
- Gesprächsdatenerfassung
- Hotline-Ziele
- Infotexte, Abwesenheitstexte
- Interne Gespräche
- Internes Telefonbuch
- KDS-Ausdruck
- Nachtschaltung
- Parkposition
- Verkehrsbeziehungsgruppen
- Voice Mail
- Wahlkontrolle

Das Kommunikationssystem kann als Gemeinschaftsanlage eingesetzt und dadurch gleichzeitig von mehreren Firmen genutzt werden. Die Funktionalität aller Leistungsmerkmale bleibt für alle Teilnehmer unverändert erhalten.

Eine Ausnahme bilden bestimmte Ressourcen, die auf die Unterbetreiber (Firmen) aufgeteilt werden müssen. Diese können entweder einem, mehreren oder allen Unterbetreibern zugeordnet werden. Bei den aufzuteilenden Ressourcen handelt es sich um:

- Teilnehmer
- Richtungen
- Vermittlungsplatz
- Abwurfstation

- Ansagegeräte, Voice Mail
- Verkehrsbeziehungsgruppen
- Türöffner
- DISA-Leitungen

Über die VBZ-Gruppen wird die Erreichbarkeit der Unterbetreiber untereinander festgelegt.

Für jeden Teilbereich lassen sich eigene Hotline-Ziele einrichten.

Abhängigkeiten

Thema	Abhängigkeiten
GEZ	Es existiert nur eine zentrale Gebührenerfassung für alle Teilbereiche.
Interne Gespräche	Interne Gespräche zwischen Teilnehmern "unterschiedlicher" Teilbereiche sind möglich, sofern dies die VBZ erlaubt.
LCR	Die automatische Leitungsbelegung ist nur systemweit konfigurierbar.
KDS-Ausdruck	Der Ausdruck der Datenbasis erfolgt nur für das gesamte System.
Internes Telefonbuch	Es werden die Namen aller Teilnehmer und Kurzwahlnummern im System angezeigt.
Vermitteln	Das Vermitteln unbewählter Leitungen ist nicht möglich.
Abwurf	Abwurf ist nur systemweit programmierbar.

15.6.1 Kurzwahl zentral in Gemeinschaftsanlagen

Mit Kurzwahl zentral in Gemeinschaftsanlagen können Kurzwahlziele in Abhängigkeit von den Verkehrsbeziehungsgruppen ausgewählt werden. Dazu kann über das WBM ein Bereich von Kurzwahlzielen den entsprechenden Verkehrsbeziehungsgruppen zugeordnet werden.

Abhängigkeiten

Thema	Abhängigkeiten
Ext. Rufnummern	Kurzwahlziele können nur externe Rufnummern enthalten.
	Die externe Rufnummer muss mit Richtungs- bzw. Belegungskennzahl eingegeben werden.
KWZ Namen	Jedem Kurzwahlziel kann ein Name zugeordnet werden.
Türsprechstelle	Die Türsprechstelle kann kein Kurzwahlziel anrufen.
VBZ-Gruppen	Es ist nicht möglich, mehrere Kurzwahlziel-Bereiche einer VBZ-Gruppe zuzuordnen.

16 Attendants

OpenScape Business bietet Vermittlungsfunktionen für jeden Bedarf, wie AutoAttendants, Telefon- und PC-basierte Attendants.

Übersicht über die angebotenen Attendants

	Einsetzbar für:	Hardware	Lizenz
AutoAttendants			
Company AutoAttendant (UC Smart)	UC Smart	Mainboard	erforderlich
Company AutoAttendant (UC Suite)	UC Suite	UC Booster Card oder UC Booster Server	erforderlich
IVM		Xpressions Compact Baugruppe	keine Lizenz erforderlich
Telefon-basierte Attendants			
OpenStage Attendant			
PC-basierte Attendants			
OpenScape Business Attendant	UC Smart	PC und Telefon, UP_{0E}	erforderlich
- OpenScape Business BLF	UC Smart	IP-Basis	
- BLF-Server	UC Smart	IP-Basis	eigene Lizenz erforderlich
myAttendant	UC Suite	UC Booster Card oder UC Booster Server	erforderlich

16.1 AutoAttendant

Der AutoAttendant bildet zusammen mit der Voicemail einen integrierten automatischen Vermittlungsdienst und einen Nachrichtenspeicher, z. B. für die Firmenzentrale. Der AutoAttendant spielt Anrufern eine Begrüßungsansage vor. Während oder nach dieser Ansage kann der Anrufer automatisch oder durch Eingabe von Ziffern an eine Nebenstelle oder Mailbox weitervermittelt werden.

Hierzu stehen verschiedenste Funktionen zur Verfügung, die mit Hilfe von Ansagen eine individuelle Vermittlung ermöglichen, wie z. B. "Drücken Sie die 1 für Service und die 2 für Vertrieb". Der Anrufer wird nach Eingabe der gewünschten Ziffer automatisch mit Vertriebs- oder Service-Mitarbeitern verbunden.

Der Company AutoAttendant ist keiner internen Rufnummer zugeordnet, sondern eine zentrale Instanz. Einer Nebenstelle können somit mehrere Company AutoAttendants bzw. Mailboxen zugewiesen werden. Dadurch ist es dem Benutzer möglich, individuell auf den entsprechenden Company AutoAttendant umzuleiten. Dem Anrufer wird je nach Umleitung entweder die Ansage der persönlichen Mailbox angesagt oder die zentrale Firmenansage. Durch den

Company AutoAttendant ist es aber auch möglich, pro Nebenstelle individuelle Ansagen abzuspielen, unabhängig von der persönlichen Mailbox.

Funktionsübersicht

- Abwurf nach Ansage zu einem konfigurierten Ziel
- Statusabhängige Ansage - es können je nach Status der Nebenstelle (frei oder besetzt) unterschiedliche Ansagen abgespielt werden.
- Unterschiedliche Tag-/Nacht-Ansage (Umschaltung erfolgt entweder manuell oder automatisch)
- Zentrale Kalendersteuerung über die Automatische Nachtschaltung
- Nachwahl einer beliebigen Rufnummer bis zu einer konfigurierten Länge (deaktivierbar)
- Kurzwahl (= Direktwahl von extern) zu konfigurierten Zielen (beliebige Rufnummer oder Mailbox)
  Insgesamt sind 4 Listen mit insgesamt 10 Zielen und einem Abwurfziel möglich. Die aktive Liste wird durch die gewählte Begrüßung festgelegt.
- Nachwahl einer beliebigen Rufnummer bis zu einer konfigurierten Länge. Die Funktion der Nachwahl kann auch deaktiviert werden um Gebührenmissbrauch zu verhindern.
- Multi Step AutoAttendant
  AutoAttendant-Mailboxen können als Kurzwahlziele (Manuell 1 bis 4, Tag/Nacht) konfiguriert werden. Dies ermöglicht eine Verkettung von Mailboxen. Dabei verhält sich der Company AutoAttendant wie bei einer Anrufumleitung, das Gespräch wird von einer verketteten Mailbox auf die nächste weitergeleitet und dabei immer die jeweilige Ansage abgespielt. Insgesamt sind bis zu 100 AutoAttendant-Mailboxen verfügbar.
- Schnellwahl
  Ansagen können deaktiviert werden, um eine schnelle Vermittlung zu garantieren.
- Ansage vor Melden mit Parallelsignalisierung (ohne Kurzwahl)
  Wird dem Anrufer die Begrüßungsansage vorgespielt, wird der Anruf beim Teilnehmer zugleich akustisch (und optisch) signalisiert. Hebt der Teilnehmer ab, wird die Ansage abgebrochen und der Teilnehmer mit dem Anrufer verbunden. Hebt der Teilnehmer nicht ab, wird die Ansage im Endlos-Betrieb abgespielt, bis der Teilnehmer auflegt oder über das Call Management weitervermittelt wird.
- Besetzttonerkennung
- Weiterleitung von Faxanrufen (automatische Faxtonerkennung) an ein vorkonfiguriertes Fax-Ziel.
- Wiederanruf
  Bei einem Wiederanruf (ausgenommen bei einem Faxanruf), wird der Anrufer zur zugehörigen Mailbox weitergeleitet, falls eine solche vorhanden ist und die Nachrichtenaufzeichnung aktiv ist.

HINWEIS: Um einen automatischen Abwurf zum Vermittlungsplatz durch das Voicemailsystem zu gewährleisten ist zwingend die Platzkennzahl intern einzutragen (Default 9, USA 0).

HINWEIS: Die Administration (TUI) einer AutoAttendant-Mailbox kann nur von einem Telefon ausgeführt werden. Deswegen sollte sich das Passwort für die AutoAttendant-Mailbox sich vom Passwort für die persönliche Mailbox des Telefons unbedingt unterscheiden!

Anwendunsbeispiele

- Beispiel 1: **Unabhängige Bereitschafts- oder Notdienste Ansagen**
  Außerhalb der Geschäftszeiten leitet der Kunde auf den AutoAttendant um (z. B. per Nachtschaltung). Der AutoAttendant verbindet auf Wunsch zum jeweils diensthabenden Servicetechniker oder bietet an, eine Nachricht in einer zentralen Mailbox zu hinterlassen. In diesem Fall führt eine Ansage zur Weiterleitung auf die verschiedenen Mobiltelefon-Nummern der Servicetechniker.
- Beispiel 2: **Unterschiedliche Sonntagsdienste für Arztpraxen**
  Der jeweils aktuelle Sonntagsdienst muss nicht mehr auf den Anrufbeantworter gesprochen bzw. die AB-Kassette gewechselt werden. Der Kunde richtet sich genauso viele AutoAttendants ein, wie er Vertreter hat. Die AutoAttendants werden einmal besprochen und jeweils am Wochenende mit einer Umleitung (Nachtschaltung) zu dem betreffenden AutoAttendant aktiviert. Hier ist es umgekehrt: Mehrere unterschiedliche Ansagen führen auf dieselbe Mailbox.

16.1.1 Company AutoAttendant (UC Smart)

Der Company AutoAttendant (UC Smart) ist der AutoAttendant der UC-Lösung UC Smart. Er kann als persönlicher AutoAttendent und als zentraler AutoAttendant verwendet werden. Die erstmalige Einrichtung erfolgt über das WBM, anschließend kann er über das Telefon gesteuert und konfiguriert werden.

Der Company AutoAttendant (UC Smart) kann in zwei Modi betrieben werden:

- **Persönlicher AutoAttendant**
  Der persönliche AutoAttendant ist einem Teilnehmer oder einer Gruppe zugeordnet und reagiert auf die Rufnummer des ursprünglich angerufenen, umleitenden Teilnehmers oder Gruppe (z.B. `12345678-100`).
  Der persönliche AutoAttendant wird über den Sammelanschluss "Voicemail" (Standardrufnummer: 351) erreicht. Der Betrieb erfolgt über SmartVM-Ports (EVM Ports) vom Typ "PhoneMail", die alle diesem Sammelanschluss zugewiesen sein müssen.
  Der Parallelbetrieb mit UC Suite ist nicht möglich.

- **Zentraler AutoAttendant**
  Der zentrale AutoAttendant wird als zentraler Vermittlungsplatz genutzt und reagiert auf seine eigene Rufnummer (z.B. `12345678-0`). Egal ob der Anruf direkt auf den AutoAttendant erfolgt oder ob der Anruf umgeleitet wurde, das Verhalten ist immer identisch.
  Der zentrale AutoAttendant wird über einen oder mehrere eigene Sammelanschlüsse erreicht (Standardrufnummer: 352). Der Betrieb erfolgt über SmartVM-Ports (EVM Ports) vom Typ "Standard", die einem oder mehreren Sammelanschlüssen (max.100) zugewiesen sein können.
  Im Default ist ein Company Auto Attendant (Gruppenindex 3) mit 2 SmartVM-Ports eingerichtet. Die Namen und die Typen der Ports können mit dem Wizard Zentrale Telefonie > SmartVM geändert werden (siehe auch *Wie Sie die Sprachbox / SmartVM konfigurieren*).
  Die Kurzwahlliste und der Begrüßungs-Upload können im Experten-Modus Telefonie > Anschaltungen > SmartVM geändert werden (siehe *Wie Sie einzelne Begrüßungen laden, sichern und löschen*). Ebenfalls können weitere (max. 99) Company AutoAttendants (UC Smart) eingerichtet und aktiviert werden.
  Der Parallelbetrieb mit UC Suite ist möglich.

Der Company AutoAttendant (UC Smart) ist lizenzpflichtig (Lizenz Company AutoAttendant). Wenn keine Lizenz vorhanden ist, werden die "Regeln" des Company AutoAttendant ignoriert, Anrufe werden zum zentralen Abwurfplatz weitergeleitet.

16.1.1.1 Wie Sie einen eingerichteten Company AutoAttendant konfigurieren

Als Beispiel soll tagsüber eine Ansage vor dem Melden mit Aufnahmemöglichkeit (z. B. Mailbox 100) eingerichtet werden. Nachts soll direkt nach der entsprechenden Ansage ein Abwurf zur Nachtbox mit Aufnahmemöglichkeit (auch Mailbox 100) erfolgen.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.
- UC Smart ist aktiviert.
- Standardmäßig erfolgt nach der Ansage im Tag- und Nacht-Betrieb ein Abwurf zum Abwurfplatz.
- Standardmäßig sind die Speeddial-Funktion und die Nachwahl nicht aktiviert.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telephonie > Anschaltung**.

3) Klicken Sie im Menübaum auf **Anschaltung > SmartVM**.

4) Klicken Sie im Menübaum auf **AutoAttendant**.

5) Deaktivieren Sie in der Zeile des gewünschten AutoAttendant (z. B. 352) das Kontrollkästchen **Abwurf nach Ansage**, um während der Begrüßungsansage Kurzwahlziffern eingeben zu können.

6) Aktivieren Sie das Kontrollkästchen **keine Nachwahl**. Somit ist nur die Eingabe vom Kurzwahlziffern möglich (keine Eingabe von internen Rufnummern möglich).

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

8) Klicken Sie im Menübaum auf **AutoAttendant** und anschließend auf den Eintrag des gewünschten AutoAttendant (z. B. 352).

9) Klicken Sie auf die Registerkarte **Kurzwahl-/Abwurfziel (Tag) bearbeiten**.

10) Wählen Sie in der Zeile **Kurzwahl 0** aus der Aufklappliste **Auswählen** den Teilnehmer für den Abwurfplatz aus (z. B. Teilnehmer 100) und in der Aufklappliste **Typ** den Eintrag **Mailbox**.

11) Wählen Sie in der Zeile **Abwurf** aus der Aufklappliste **Auswählen** den Teilnehmer für den Abwurfplatz aus (z. B. Teilnehmer 100).

12) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

13) Klicken Sie auf die Registerkarte **Kurzwahl-/Abwurfziel (Nacht) bearbeiten**.

14) Wählen Sie in der Zeile **Abwurf** aus der Aufklappliste **Auswählen** den Teilnehmer für den Abwurfplatz aus (z. B. Teilnehmer 100) und in der Aufklappliste **Typ** den Eintrag **Mailbox**.

15) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

16) Klicken Sie im Menübaum auf **SmartVM**.

17) Um bei der Abwurf-Mailbox eine zweifache Begrüßung zu vermeiden, wählen Sie in der Zeile des Abwurfplatzes (z. B. Teilnehmer 100) aus der Aufklappliste **Begrüßung** den Eintrag **Kein** aus. Dann erfolgt direkt nach der Begrüßung des Company AutoAttendant der Signalton für die Aufnahme.

18) Die die Begrüßung des Company AutoAttendant kann über ein Telefon oder über den Experten-Modus > Wartung > SmartVM geändert werden (siehe *Konfiguration der Sprachbox / SmartVM*).

16.1.1.2 Wie Sie einen neuen Company AutoAttendant einrichten

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.
- UC Smart ist aktiviert.
- Erforderliche Lizenzen

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Konfigurieren Sie zuerst den Sammelanschluss:

a) Klicken Sie im Navigationsbaum auf **Telefonie > Kommende Rufe**.

b) Klicken Sie im Menübaum auf **Kommende Rufe > Gruppen-/Sammelanschluss**.

c) Klicken Sie auf die Registerkarte **Gruppe hinzufügen**.

d) Geben Sie im Feld **Rufnummer** die Rufnummer des neuen AutoAttendant ein (z. B.`353`).

e) Geben Sie im Feld **Durchwahlnummer** die Durchwahlnummer des neuen AutoAttendant ein (z. B.`353`).

f) Geben Sie im Feld **Name** den Namen des neuen AutoAttendant ein (z. B. `AutoAttendant 353`).

g) Wählen Sie aus der Aufklappliste **Typ** den Eintrag **Zyklischer Sammelanschluss** aus.

h) Wählen Sie im Bereich **Gruppenmitglied** aus der Aufklappliste Rufnummer den gewünschten AutoAttendant Port aus (z. B. **745 SmartVM 7**).

i) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

j) Um einen weiteren AutoAttendant Port zu dem Sammelanschluss hinzuzufügen, klicken Sie im Menübaum unter **Gruppen-/Sammelanschluss** auf den gewünschten AutoAttendant und anschließend auf die Registerkarte **Mitglied hinzufügen**. Wählen Sie dort unter **Rufnummer** einen weiteren AutoAttendant Port aus (z. B. **746 SmartVM 8**) aus.

k) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

3) Konfigurieren Sie die Mailbox des AutoAttendant:

a) Klicken Sie im Navigationsbaum auf **Telephonie > Anschaltung**.

b) Klicken Sie im Menübaum auf **Anschaltungen > SmartVM**.

c) Klicken Sie im Menübaum auf **AutoAttendant**.

d) Setzen Sie in der Zeile des gewünschten AutoAttendant (z. B. `353`) die beiden Kontrollkästchen nach Bedarf:

Abwurf nach Ansage: wenn aktiviert, kann der Anrufer während der Begrüßung eine Kurzwahlziffer für eine Vermittlungsmöglichkeit eingeben.

keine Nachwahl: wenn aktiviert, können nur Kurzwahlziffern und keine internen Rufnummern eingegeben werden.

e) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

f) Klicken Sie im Menübaum auf **SmartVM**.

g) Klicken Sie auf die

h) Wählen Sie auf der Registerkarte **SmartVM-Mailboxen bearbeiten**. in der Zeile des gewünschten AutoAttendants unter **Begrüßung** die gewünschte Begrüßung aus.

i) Aktivieren Sie in der Zeile des gewünschten AutoAttendants das Kontrollkästchen **AutoAttendant**.

j) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

4) Konfigurieren Sie die Vermittlungsmöglichkeiten (z. B. "0" für Verbinden und "1" für eine Ansage):

a) Klicken Sie im Menübaum auf ***SmartVM** und anschließend auf **AutoAttendant**.

b) Klicken Sie im Menübaum unter **AutoAttendant** auf den Eintrag des gewünschten AutoAttendant (z. B. `352`).

c) Klicken Sie auf die Registerkarte **Kurzwahl-/Abwurfziel (Tag) bearbeiten**.

d) Geben Sie in der Zeile **Kurzwahl 0** unter **Rufnummer** die Rufnummer ein, zu der verbunden werden soll, und wählen Sie in der Aufklappliste **Typ** den Eintrag **Rufnummer**.

e) Wählen Sie in der Zeile **Kurzwahl 1** aus der Aufklappliste **Auswählen** den Teilnehmer für den Abwurfplatz aus (z. B. Teilnehmer 100) und in der Aufklappliste **Typ** den Eintrag **Mailbox**.

f) Wählen Sie in der Zeile **Abwurf** aus der Aufklappliste **Auswählen** den Company AutoAttendant aus (z. B. `353`).

g) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

h) Ist das Flag **keine Nachwahl** deaktiviert, können während der Begrüßungsansage auch interne Nummern gewählt werden. Um Gebührenmissbrauch zu vermeiden, sollte die **Rufnummernlängenbegrenzung** überprüft bzw. limitiert werden, damit keine externen Rufnummern gewählt werden können (siehe **Experten-Modus > Telephonie > SmartVM > SmartVM-Parameter bearbeiten**).

16.1.2 Company AutoAttendant (UC Suite)

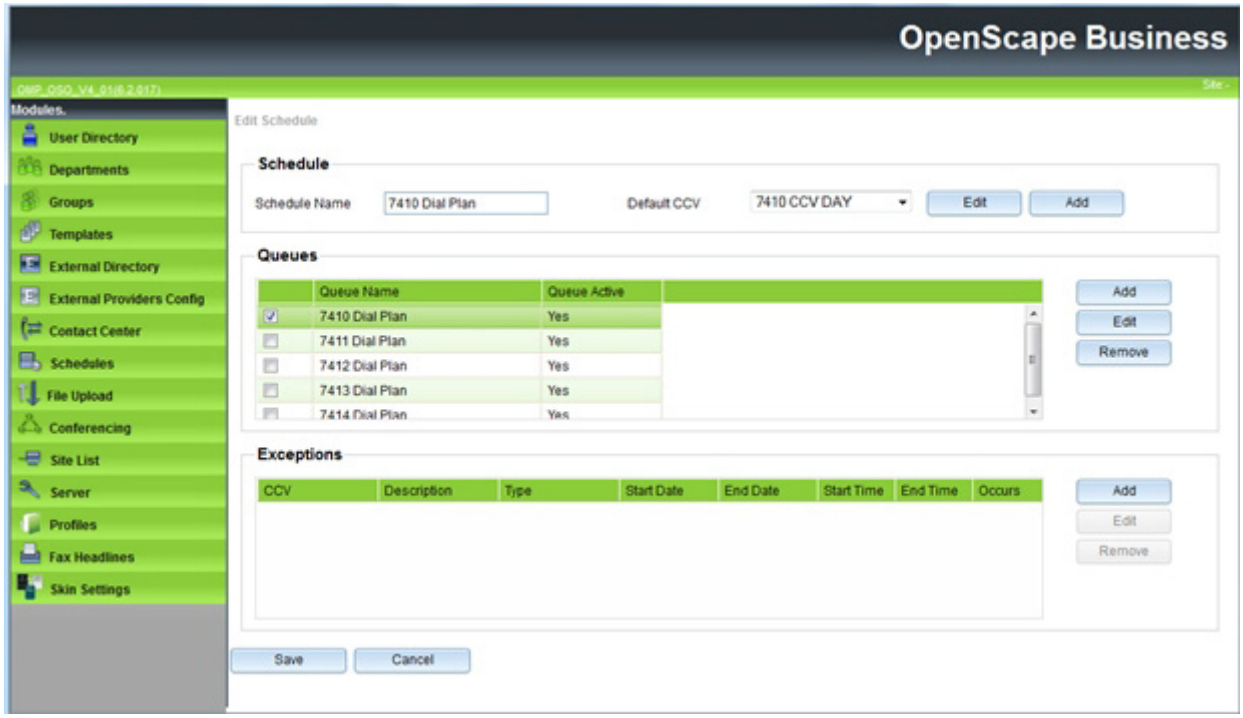
Der zentrale Company AutoAttendant (UC Suite) ist ein Vermittlungsplatz, der ausschließlich vom Administrator konfiguriert werden kann. Um die Installation und Einrichtung zu erleichtern, stehen fünf Templates zur Verfügung, die vom Administrator angepasst werden können.

Der Administrator kann den Company AutoAttendant (UC Suite) mit Hilfe von Zeitplänen regelbasiert konfigurieren. Zeitpläne ermöglichen erweiterte Auswahlmöglichkeiten wie z. B. nach Namen wählen.

16.1.2.1 Zeitpläne

Über einen Zeitplan und die darin enthaltenen Regeln (Call Control Vector CCV) wird definiert, wie kommende Anrufe an bestimmten Tagen und zu bestimmten Zeiten behandelt werden sollen.

Beispielsweise kann für Werktage eine Regel für die Frühschicht (von 6:00 Uhr bis 14:00 Uhr), eine für die Mittagschicht (14:00 Uhr bis 22:00 Uhr) und eine für die Nachtschicht (von 22:00 bis 06:00 Uhr) definiert werden. Für das Wochenende kann eine Wochenendregel definiert werden. Für jede dieser Regeln kann zum Beispiel angegeben werden, ob eine Ansage abgespielt und/ oder wohin Anrufe weitergeleitet werden sollen.



Einem Zeitplan muss mindestens eine Regel (Call Control Vector CCV) zugeordnet werden. Die Regeln bestimmen für den Zeitraum für den ein Zeitplan gilt, wie kommende Anrufe behandelt werden. Regeln gelten ausschließlich für Anrufe und nicht für Faxe und E-Mails.

Regeln werden mit dem graphischen Regel-Editor (CCV-Editor) durch die Verknüpfung von vordefinierten CCV-Objekten erstellt und können nach der Fertigstellung unter einem frei definierbaren Namen gespeichert werden.

Gespeicherte Regeln können einem oder auch mehreren Zeitplänen als Standard-Regel (Standard-CCV) oder Ausnahme-Regel (Ausnahme-CCV) zugeordnet werden. Das Öffnen, Modifizieren und erneute Speichern über den Regel-Editor ist jederzeit möglich.

Wurde einem Zeitplan eine Standard-Regel (Standard-CCV) zugeordnet, kann dieser Zeitplan unter einem frei definierbaren Namen gespeichert werden. Ein Zeitplan mit einer Standard-Regel gilt nach Zuweisung zu einer Warteschlange 24

Stunden am Tag und 365 Tage im Jahr. Sollen zu bestimmten Zeiten (Pause, Wochenende, Feiertag, Urlaub usw.) andere Regeln gelten, können diese dem entsprechenden Zeitplan als Ausnahme-Regeln (Ausnahme-CCV) zugeordnet werden. Damit kann definiert werden, wie kommende Anrufe beispielsweise während der Urlaubszeit behandelt werden sollen. Urlaubspläne haben hierbei Vorrang vor anderen Zeitplänen und Regeln.

Regel-Editor (CCV-Editor)

Mit dem Regel-Editor können aus vordefinierten CCV-Objekten Regeln gebildet werden. Die Anordnung der CCV-Objekte und deren Eigenschaften bestimmen, wie kommende Anrufe behandelt werden.

Folgende vordefinierte CCV-Objekte stehen zur Verfügung:

INFO: Für alle genannten CCV-Objekte gelten zusätzlich die beiden folgenden allgemeinen Eigenschaften:

Beschreibung: Optionale Möglichkeit das CCV-Objekt zu beschreiben, wie zum Beispiel Begrüßungsansage.

Aktion nach Zifferneingabe: Angabe der benötigten Ziffer(n) ohne Leerzeichen, Kommas oder anderer Zeichen. Die Angabe bezieht sich auf das vorherige CCV-Objekt. Wurde dort unter Mögliche Ziffern 9 angegeben, muss auch hier 9 stehen.

- **Nachricht abspielen**
  Bewirkt das Abspielen der gewünschten Ansage. Ausgewählt werden kann eine in der UC Suite vorliegende Audiodatei. Darüber hinaus kann eine neue Audiodatei in die UC Suite importiert werden oder eine neue Ansage aufgezeichnet und anschließend als Audiodatei in die UC Suite importiert werden.
  Durch das Abspielen der Ansage wird jeweils ein Media Stream Channel belegt.
  Eigenschaften:
  - **Dateiname**: Auswahl einer Ansage (Audiodatei im wav-Format)
  - **Abbruchtasten**: Angabe einer Taste oder Tastenkombination auf der Wähltastatur, mit der ein Anrufer das Abspielen der Ansage abbrechen kann.
  - **Datei-Manager**: Über diese Schaltfläche ist es direkt möglich, eine Audio-Datei im wav-Format hochzuladen bzw. mit dem Aufzeichnungsgerät eine neue Sprachdatei zu erzeugen.
- **Verbindung mit Anrufer trennen**
  Bewirkt das Beenden der Verbindung
  Nach diesem CCV-Objekt kann kein weiteres CCV-Objekt mehr eingefügt werden.
- **Zu CCV**
  Bewirkt eine Schleife zu einem anderen CCV-Objekt
  Eigenschaft:
  - **Ziel-CCV**: Auswahl des CCV-Objekts

- **Aktion nach Zifferneingabe ausführen**
  Bewirkt die Ausführung des oder der nachfolgenden CCV-Objekte in Abhängigkeit von den dort angegebenen Ziffern (Aktion nach Zifferneingabe).
  Eigenschaften:
  - **Dateiname**: Auswahl einer oder mehrerer Ansagen (Audiodatei im wav-Format)
  - **Wiedergabeliste**: Liste der ausgewählten Ansagen (Audiodatei im wav-Format) in der Reihenfolge der Wiedergabe
  - **Zeitüberschreitung bei Zifferneingabe**: Zeit in Sekunden, innerhalb der das Kommunikationssystem auf die Zifferneingabe wartet.
    Erfolgt die vollständige Zifferneingabe nicht innerhalb der angegebenen Zeit, wird die Nachricht (Ansage) erneut abgespielt.
  - **Link an**: Auflistung der Ziffer mit Ziel.
    Die Ziffern und Ziele können hinzugefügt, bearbeitet und entfernt werden.
  - **Datei-Manager**: Über diese Schaltfläche ist es direkt möglich, eine Audio-Datei im wav-Format hochzuladen bzw. mit dem Aufzeichnungsgerät eine neue Sprachdatei zu erzeugen.

  Der Inhalt der Wiedergabeliste wird im Regel-Editor anhand eines Tooltips angezeigt, wenn man mit dem Mauszeiger auf dem CCV-Objekt verweilt.
- **Einzelschritt-Übergabe**
  Die Funktion ist abhängig von der Einstellung **Normales Vermittlungsplatz-SST** (WBM, **Experten-Modus**: **Applikationen > OpenScape Business UC Suite > Server > Allgemeine Einstellungen**):
  - **Normales Vermittlungsplatz-SST** aktiviert (Standardeinstellung, nicht für USA): Bewirkt die Übergabe des Anrufs, unabhängig davon, ob das Ziel frei, besetzt oder nicht verfügbar ist.

    INFO: Bei einem Teilnehmer mit Anklopfschutz wird der Anruf erst vermittelt, wenn der Zielteilnehmer frei ist. Ein Anklopfen im Besetztfall erfolgt nicht.

  - **Normales Vermittlungsplatz-SST** deaktiviert (Standardeinstellung, nur für USA): Bewirkt eine Übergabe des Anrufs, wenn das Ziel frei ist.
    Ist das Ziel besetzt und der Anklopfschutz deaktiviert oder ist das Ziel nicht verfügbar, wird dem Anrufer eine Ansage eingespielt. Dabei kann der Anrufer wählen, ob er eine Nachricht auf der Sprachbox des Teilnehmers hinterlassen möchte oder ob er die Rufnummer eines anderen Ziels wählen möchte.
    Ist das Ziel besetzt und der Anklopfschutz aktiviert, erfolgt keine Vermittlung des Anrufs.

  Nach diesem CCV-Objekt kann kein weiteres CCV-Objekt mehr eingefügt werden.
  Eigenschaft:
  - **Zielnebenstelle**: Angabe der internen Rufnummer oder der externen Durchwahl mit Amtsleitungsnummer. Leerzeichen, Kommas oder andere Zeichen sind nicht erlaubt.

  Die Rufnummer der Zielnebenstelle wird im CCV-Objekt angezeigt.

- **In Mailbox aufzeichnen**
  Bewirkt den Anruf an die gewünschte Sprachbox eines Teilnehmers oder einer Sprachbox-Gruppe
  Nach diesem CCV-Objekt kann kein weiteres CCV-Objekt mehr eingefügt werden.
  Eigenschaft:
  – **Benutzer-Mailbox**: Angabe der Rufnummer der Sprachbox eines Teilnehmers oder einer Sprachbox-Gruppe

  Die Rufnummer und der Name der Sprachbox oder der Sprachbox-Gruppe werden im Regel-Editor anhand eines Tooltips angezeigt, wenn man mit dem Mauszeiger auf dem CCV-Objekt verweilt.
- **Übergabe nach Melden**
  Bewirkt die Übergabe des Anrufs an ein internes Ziel. Während der Übergabe wird dem Anrufer Wartemusik (Music On Hold MOH der UC Suite) eingespielt.
  Im Gegensatz zum CCV-Objekt Einzelschritt-Übergabe müssen hier zwei weitere CCV-Objekte eingefügt werden. Es muss nämlich definiert werden, wie sich das Kommunikationssystem verhalten soll, wenn das Anrufziel besetzt ist oder der Anruf nicht angenommen wird. Üblicherweise wird dem Anrufer in diesen Fällen eine Ansage eingespielt.
  Eigenschaften:
  – **Zielnebenstelle**: Angabe der internen Rufnummer.
    Es werden nur interne Rufnummern im eigenen Knoten unterstützt. Das Weiterleiten auf externe Ziele, virtuelle Teilnehmer, weitere AutoAttendants, UCD inkl. Contact Center, Mobility Teilnehmer sowie externe CallMe-Ziele ist nicht zulässig! Für diese Szenarien ist der SST (Einzelschritt Übergabe) zu verwenden.
  – **Zeitüberschreitung beim Klingeln**: Zeit in Sekunden, innerhalb der der Anruf angenommen werden muss.
    Wird der Anruf nicht innerhalb der angegebenen Zeit angenommen, wird dieser zum Kommunikationssystem zurückgestellt und das nächste CCV-Objekt verwendet.

    INFO: Die hier angegebene Zeit muss kürzer sein als die für die Rufweiterschaltung konfigurierte Zeit (Standardeinstellung für die Rufweiterschaltung = 15 Sekunden). Siehe *Administratordokumentation, Funktionen am Telefon*.

  – **Anruf zurücknehmen, wenn Zielgerät weitergeleitet/umgeleitet ist**: Option (gilt nur für interne Rufnummer)
    Bei aktivierter Option erfolgt eine Prüfung des Anrufziels. Wurde für das Anrufziel eine Anrufweiterschaltung oder Anrufumleitung aktiviert, wird der Anruf zum Kommunikationssystem zurückgestellt und das nächste CCV-Objekt verwendet.
  – **Anwesenheitsstatus bei der Anrufübergabe prüfen**: Option
    Bei aktivierter Option erfolgt eine Prüfung des Anwesenheitsstatus des Anrufziels. Bei einem anderen Anwesenheitsstatus als Büro wird auf die Sprachbox des Anrufziels umgeleitet.

- **Nach Name wählen**
  Bewirkt die Aufforderung des Anrufers, die ersten drei Buchstaben des gewünschten Teilnehmer-Nachnamens über die Wähltastatur einzugeben.
  Gibt es einen Teilnehmer mit den eingegebenen Anfangsbuchstaben, wird eine Verbindung hergestellt.
  Gibt es mehrere Teilnehmer mit den eingegebenen Anfangsbuchstaben, werden dem Anrufer die Namen dieser Teilnehmer angesagt (maximal 10 Teilnehmer). Hat ein Teilnehmer keine Namensansage aufgezeichnet, wird stattdessen die Rufnummer angesagt. Nach der Auswahl des gewünschten Teilnehmers wird eine Verbindung hergestellt.
  Entspricht kein Teilnehmer den eingegebenen Anfangsbuchstaben, erhält der Anrufer eine entsprechende Meldung.

  INFO: Die Tasten der Wähltastatur reagieren auf den ersten Tastendruck. Mit jedem Tastendruck wird geprüft, ob es Teilnehmer-Nachnamen mit den der Taste zugeordneten Buchstaben gibt.

  Beispiel: Im internen Verzeichnis gibt es die folgenden fünf Nachnamen mit den Anfangsbuchstaben t, u und v: Taylor, Taler, Ullrich, Vasquez und Volterra. Um ein Verbindung mit dem Teilnehmer Taylor herzustellen, sind folgende Tasten zu betätigen: 8 2 9

  Nach diesem CCV-Objekt kann kein weiteres CCV-Objekt mehr eingefügt werden.
  Eigenschaften:
  - **Methode**: Auswahl von **An Nebenstelle übergeben** oder **In Mailbox aufzeichnen**.
    Je nach ausgewählter Methode wird eine Verbindung zum gewünschten Teilnehmer oder zu dessen Sprachbox hergestellt. Dabei werden ausschließlich interne Teilnehmer unterstützt, die mit Vor- und Nachnamen im internen Verzeichnis eingetragen sind.
- **Nebenstellenwahl**
  Bewirkt die Aufforderung des Anrufers, die Rufnummer des gewünschten Teilnehmers über die Wähltastatur einzugeben.
  Wählt der Anrufer die Rufnummer eines virtuellen Teilnehmers, wird er aufgefordert eine andere Teilnehmer-Rufnummer einzugeben. Anschließend wird eine Verbindung hergestellt. Meldet sich der gewünschte Teilnehmer nicht, nimmt dessen Sprachbox den Anruf entgegen.
  Nach diesem CCV-Objekt kann kein weiteres CCV-Objekt mehr eingefügt werden.
  Eigenschaften:
  - **Methode**: Auswahl von **An Nebenstelle übergeben** oder **In Mailbox aufzeichnen**.
    Je nach ausgewählter Methode wird eine Verbindung zum gewünschten Teilnehmer oder zu dessen Sprachbox hergestellt. Dabei werden ausschließlich interne Teilnehmer unterstützt, deren Rufnummer im internen Verzeichnis eingetragen ist.

- **Sprache einstellen**
  Bewirkt die Auswahl der Sprache für die jeweilige Standardansage anhand der Rufnummer des Anrufers. Zu beachten ist, dass ausschließlich Standardansagen (Systemansagen) und keine persönlichen Ansagen berücksichtigt werden.
  Definiert werden kann zum Beispiel, dass für eine Rufnummer mit der Ländervorwahl 0049 eine deutsche Ansage und für eine Rufnummer mit der Ländervorwahl 0033 eine französische Ansage abgespielt wird.
  Eigenschaften:
  - **Standard-Sprache**: Aufklappliste zur Auswahl einer Sprache.
    Die hier ausgewählte Sprache wird für alle Rufnummern verwendet, für die selbst keine Sprache definiert wurde.
  - **Muster**: Angabe der Rufnummer, der eine bestimmte Sprache zugeordnet werden soll.
    Folgende Platzhalter können verwendet werden: * = beliebige Zahl, ? = beliebige Ziffer.
  - **Sprache**: Aufklappliste zur Auswahl der Sprache, die der zugehörigen Rufnummer (**Muster**) zugeordnet werden soll.

  Beliebig vielen verschiedenen Rufnummern (**Muster**) kann eine Sprache zugeordnet werden.
- **CLI Routing**
  Bewirkt die Weiterleitung eines Anrufs an ein oder mehrere, aufeinander folgende CCV-Objekte anhand der Rufnummer des Anrufers.
  Definiert werden kann zum Beispiel, dass für eine Rufnummer mit der Ländervorwahl 0049 zuerst eine deutsche Ansage abgespielt werden soll (CCV-Objekt **Nachricht abspielen**) und der Anruf anschließend an eine internes Telefon weitergeleitet werden soll (CCV-Objekt **Einzelschritt-Übergabe**).
  Eigenschaften:
  - **Standard**: Aufklappliste zur Auswahl des CCV-Objekts.
    Das hier ausgewählte CCV-Objekt wird für alle Rufnummern verwendet, für die selbst kein Ziel definiert wurde.
  - **Muster**: Angabe der Rufnummer, der ein bestimmtes CCV-Objekt als Ziel zugeordnet werden soll.
    Folgende Platzhalter können verwendet werden: * = beliebige Zahl, ? = beliebige Ziffer.
  - **Beschreibung**:
    Angabe einer Erläuterung.
    Für das **Muster** 0049 (= Ländervorwahl Deutschland) kann zum Beispiel Deutschland eingegeben werden.
    Der hier eingegebene Text wird im Regel-Editor angezeigt.
  - **Ziel**: Aufklappliste zur Auswahl des CCV-Objekts, das der zugehörigen Rufnummer (**Muster**) als Ziel zugeordnet werden soll.

  Beliebig vielen verschiedenen Rufnummern (**Muster**) kann ein CCV-Objekt als Ziel zugeordnet werden.

- **Bedingte Verzweigung**
  Bewirkt die Weiterleitung eines Anrufs an ein oder mehrere, aufeinander folgende CCV-Objekte anhand einer Bedingung.
  Definiert werden kann zum Beispiel, dass Anrufern eine Ansage eingespielt wird (Bitte rufen Sie zu einem späteren Zeitpunkt noch einmal an ...), sobald sich mehr als 20 Anrufe in einer Warteschlange befinden.
  Eigenschaften:
  - **Variable**: Auswahl von **Anrufe** oder **Verfügbare Agenten**.
    Je nach ausgewählter Variablen wird als Bedingungsvorgabe die Anzahl der wartenden Anrufe in einer Warteschlange oder die Anzahl der verfügbaren Agenten (inklusive Agenten in der Nachbearbeitungszeit) einer Warteschlange verwendet. In der zugehörigen Aufklappliste ist die Bedingung (**kleiner als**, **größer als**, **kleiner oder gleich als**, **größer oder gleich als**, **gleich als**) auszuwählen und in dem zugehörigen Eingabefeld ist der Vergleichswert einzugeben.
  - **Bedingung erfüllt**: Aufklappliste zur Auswahl des CCV-Objekts, das bei erfüllter Bedingung als Ziel verwendet werden soll.
  - **Bedingung nicht erfüllt**: Aufklappliste zur Auswahl des CCV-Objekts, das bei nicht erfüllter Bedingung als Ziel verwendet werden soll.

  Die Anzahl der verfügbaren Agenten in einer Warteschlange wird durch folgende Statusänderungen der Agenten beeinflusst:
  - Anmelden eines Agenten in die Warteschlange über "Anmelden/Login": --> +1
  - Abmelden eines Agenten aus der Warteschlange über "Abmeldung/ Logout": --> -1
  - Agent im Zustand "Pause": --> -1
  - Agent im Zustand "Verfügbar nach Pause": --> +1

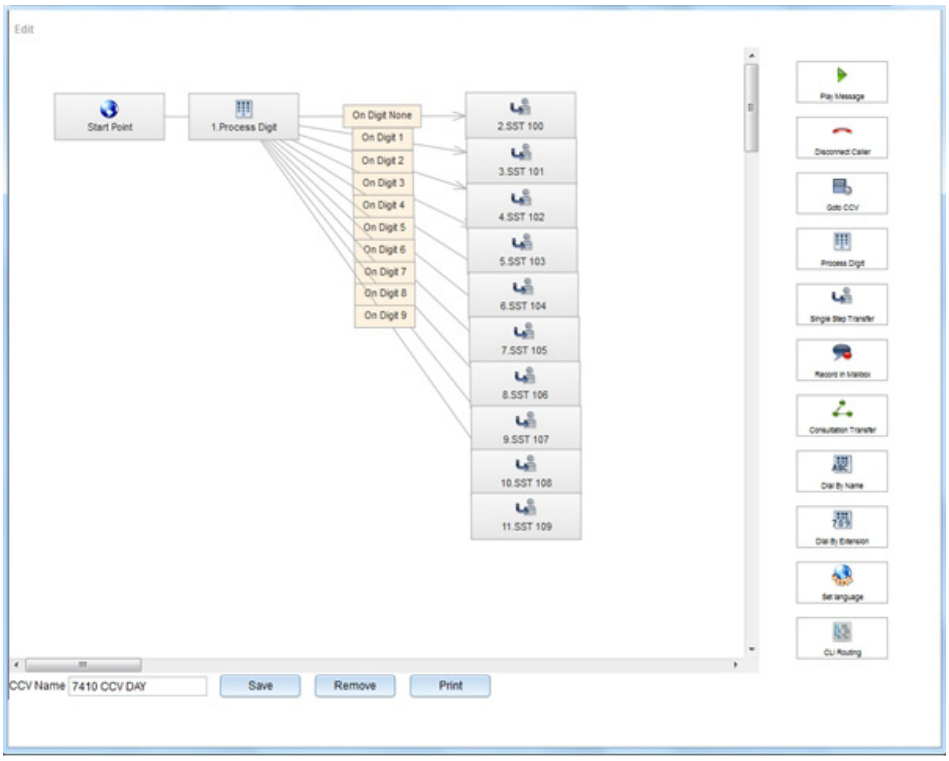
  Die Anzahl der verfügbaren Agenten in einer Warteschlange wird durch folgende Statusänderungen der Agenten **nicht** beeinflusst:
  - Agent im Zustand "Klingeln"
  - Agent im Zustand "Gespräch"
  - Agent in Zustand "Nachbearbeitung"
  - Agent im Zustand "Verpasster Anruf"
  - Agent im Zustand "Überfällig"

16.1.2.2 Templates

Die nachfolgenden Template sind vorbelegte, standardisierte Vorlagen für den Company AutoAttendant (UC Suite), die beliebig verändert und an den speziellen Bedarf angepasst werden können.

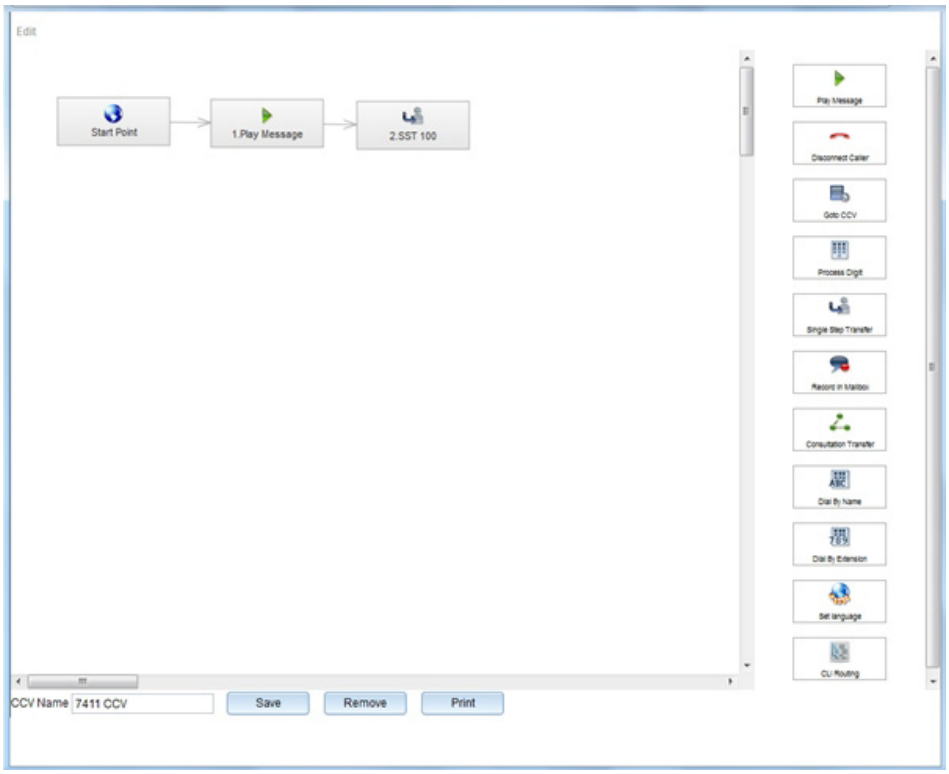
Template 1 - 7410 CCV: Anruf mit Durchschaltung (ohne Mailbox)

Dem Anrufer wird eine Ansage vorgespielt. Anschließend wird er aufgefordert eine (Ziffer) Taste zu drücken und wird zu einem Teilnehmer durchgestellt. Drückt der Anrufer keine Taste, wird er zum Abwurfplatz (Default 100) durchgestellt.



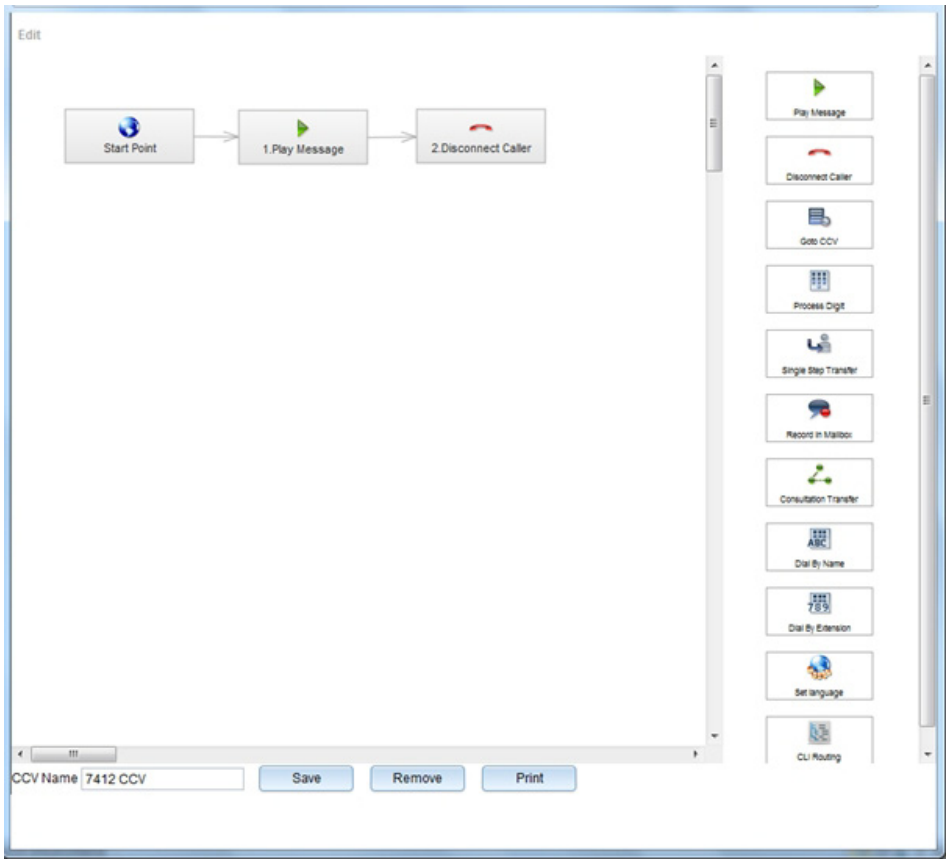
Template 2 - 7411 CCV: Ansage vor dem Melden

Dem Anrufer wird eine Ansage vorgespielt. Anschließend wird auf den Abwurfplatz 100 vermittelt.



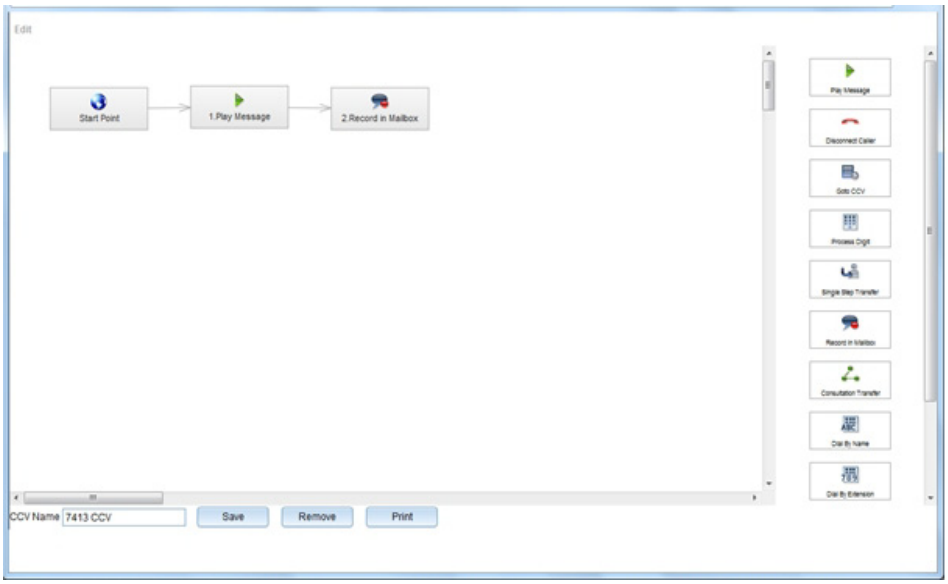
Template 3 - 7412 CCV: Anruf außerhalb der Geschäftszeit

Dem Anrufer wird bei einem eingehenden Anruf außerhalb der Geschäftszeiten eine Ansage vorgespielt. Anschließend wird die Verbindung getrennt.



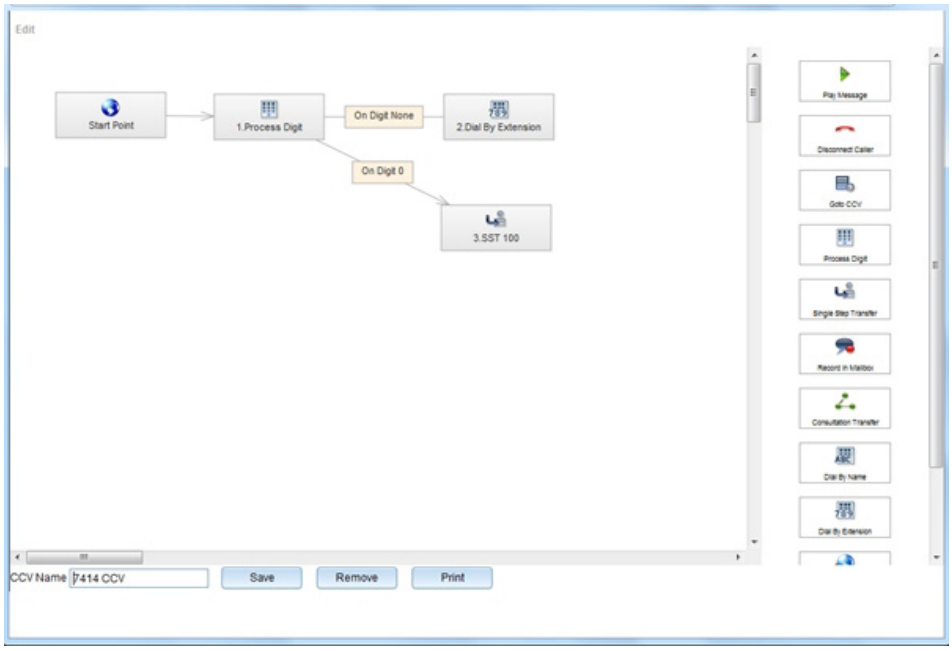
Template 4 - 7413 CCV: Anruf außerhalb der Geschäftszeit mit Rufweiterschaltung auf eine Mailbox

Dem Anrufer wird bei einem eingehenden Anruf außerhalb der Geschäftszeiten eine Ansage vorgespielt. Anschließend wird er aufgefordert auf eine Mailbox zu sprechen und kann eine Nachricht hinterlassen.



Template 5 - 7414 CCV: Dial by Extension USA Feature

Dem Anrufer wird eine Ansage vorgespielt. Gibt er anschließend keine weiteren Ziffern ein, wird er auf das CCV Dial by Extension (Nebenstellenwahl) weitervermittelt. Drückt er die Ziffer 1, wird er auf den Abwurfplatz (Default 100) vermittelt.



16.1.3 Xpressions Compact

Xpressions Compact bietet eine integrierte AutoAttendant-Lösung für Ihr Kommunikationssystem. Bis zu 500 Mailboxen mit einer Aufnahmekapazität von 100 Stunden stehen zur Verfügung.

Die AutoAttendant-Mailbox bietet neben der Vermittlungsmailbox auch die Möglichkeit der Nachrichtenaufzeichnung. Eingehende Anrufe können weitergeleitet werden an:

- eine beliebige Nebenstelle
- eine Teilnehmer- oder Gastmailbox
- eine Informationsmailbox
- ein sonstiges benutzerdefiniertes Ziel, einschließlich externer Ziele
- ein abhängig von der Rufnummer vordefiniertes Ziel (10 Ziele stehen zur Verfügung; es wird in diesem Fall keine Begrüßung gespielt)
- an einen Vermittlungsplatz

Leistungsmerkmale der Xpressions Compact:

- Anrufweiterleitung zur Mailbox
- Verteilerlisten für Sprachnachrichten (20 Listen mit je 499 Zielen möglich)
- Rundsenden von Nachrichten
- Nachrichtensignalisierung
- Voice to E-Mail
- Mitschneiden von Gesprächen
- Benachrichtigungsruf (SMS und Pager möglich)
- Weiterleitung von Nachrichten per Namenswahl
- Weiterleiten von Faxanrufen
- Statistiken für Vermittlungsmailboxen
- Zentrale Voice-Mailbox
- Zugangsschutz (3 bis 8stelliges Passwort)

Weitere Information

Detaillierte Informationen können der Administratordokumentation Xpressions Compact entnommen werden

16.2 OpenStage Attendant

Vermittlungsfunktionen können mit einem speziell eingerichteten OpenStage-Telefon ausgeführt werden. Der OpenStage Attendant dient gleichzeitig als Abwurfplatz.

Am OpenStage Attendant kommen alle Gespräche an, für die keine Durchwahlmöglichkeit besteht, oder für die über die Rufzuordnungkriterien kein Teilnehmer erreicht werden konnte (Abwurf). Die Vermittlungsperson leitet die kommenden Gespräche dann zu den gewünschten Teilnehmern weiter.

Folgende OpenStage Telefone können als Attendant fungieren:

- OpenStage 30
- OpenStage 40
- OpenStage 60
- OpenStage 80

Tastenlayout

Bei einem als Vermittlungsplatz konfigurierten OpenStage Telefon sind die frei programmierbaren Funktionstasten wie folgt belegt:

- Nachtschaltung
- Telefonbuch
- Wartende Anrufe
- Aufschalten
- Halten
- Extern 1
- Extern 2 (nicht bei OpenStage 40)
- Leere, nicht vorbelegte Taste (nicht bei OpenStage 40)

16.3 OpenScape Business Attendant

Der OpenScape Business Attendant bietet Vermittlungsfunktionen sowie eine Telefonbuchanbindung für OpenScape Business. Der OpenScape Business Attendant kann bei Vernetzung mit einem BLF-Server erweitert werden, um netzweite BLF- und Presence-Informationen anzuzeigen.



Wesentliche Vermittlungsfunktionen:

- Anstehende bzw. angenommene Anrufe verwalten
- Daten des aktiven Gesprächs
- Geparkte, gehaltene Gespräche
- Anrufliste
- Journal für angenommene, verpasste und gehende Gespräche
- Persönliche VoiceMail

Telefonbuchanwendung:

- Outlook-Kontakte
- LDAP (Anschaltung via OpenDirectory Service)
- Persönliches Telefonbuch

Besetzlampenfeld-Status:

- Frei, Besetzt, Gerufen, Umgeleitet

Sichtbarkeit des Anwesenheitsstatus (netzweit ausschließlich mit BLF-Server):

- Büro, Besprechung, Krank, Pause, Außer Haus, Urlaub, Mittagspause, Zuhause
- Ändern des Anwesenheitsstatus für Teilnehmer des eigenen Knotens (derzeit nicht für Teilnehmer aus anderen Knoten)

Bei OpenScape Business Attendant stehen drei Oberflächen-Styles zur Auswahl.

Es können maximal 8 OpenScape Business Attendant je Kommunikationssystem angeschlossen werden (max. 8 Lizenzen je OpenScape Business X1/X3/X5/X8 und OpenScape Business S).

Die Lizenzierung des OpenScape Business Attendant geschieht über das WBM.

Technische Voraussetzungen

- Standard Windows PC
- Terminal Server Einsatz bei Verwendung von HFA-Telefonen möglich (Voraussetzungen dazu siehe *Voraussetzungen für UC Suite PC-Clients*)
- USB-Interface bzw. LAN-Interface, abhängig vom verwendeten Endgerät
- Bildschirm mit einer Auflösung von min. 1024x768, optional zweiter Bildschirm zur Anzeige des zweiten BLF
- Grafikkarte mit 16bit Farbtiefe (min. 256 Farben)
- Internetzugang für Support bzw. Updates

Betriebssystem

- Microsoft Windows 8
- Microsoft Windows 7
- Microsoft Windows Vista
- Microsoft Windows XP
- Microsoft Windows 2012, 2008 R2, 2008 und 2003 Server als Microsoft Terminal Server

Der Support von OpenScape Business Attendant für Microsoft Windows XP und Microsoft Windows 2003 Server endet zeitgleich mit der Betreuungseinstellung durch Microsoft. Das Produkt wird weiterhin unterstützt, jedoch nicht mehr detailliert getestet.

Unterstützte Telefone

- openStage 40 HFA, 60 HFA, 80 HFA
- openStage 30T, 40T, 60T, 80T
- optiPoint 500
- optiPoint 410/420

Einfaches Plug and Play bei der Installation

Der OpenScape Business Attendant wird bei der Ersteinrichtung über einen Wizard konfiguriert, der die erforderlichen Konfigurationsdialoge öffnet.

Z. B.:

- Abfrage des Endgeräte-Typs

- Abfrage und Überprüfung des Anlagenzugangs
- Abfrage und Überprüfung eines evtl. vorhandenen Netzverbunds
- Automatische Integration des BLFs.

16.3.1 OpenScape Business BLF

Das Besetzttlampenfeld OpenScape Business BLF ist eine eigenständige Applikation zur Anzeige von Belegtzuständen. Optionale Funktionen sind Anzeige und Setzen des Anwesenheitsstatus, sowie der Verbindungsaufbau für das zugeordnete Telefon.

Wesentliche Funktionen:

- OpenScape Business BLF ist skalierbar und individuell einrichtbar
  - 10 bis 350 BLF-Felder (Benutzerschaltflächen), abhängig von der Bildschirmauflösung
- Telefonfunktionen
  - Wählen
  - Rufnannahme
  - Trennen
- Anwesenheitsstatus setzen (für den eigenen Teilnehmer)
- Telefonbuch (Systemtelefonbuch)
- Anrufjournal
- Max. 50 gleichzeite BLF-Applikationen je OpenScape Business X1/X3/X5/X8 und OpenScape Business S

Zum Betrieb des OpenScape Business BLF ist jeweils eine Lizenz "OpenScape Business V1 BLF" erforderlich, plus eine Lizenz "UC Smart User". Alternativ ist jeweils eine Lizenz "OpenScape Business V1 BLF" erforderlich, plus eine Lizenz "UC Suite User"

Technische Voraussetzungen

- Standard Windows PC
- Betriebssystem: Windows XP (bis zur Betreuungseinstellung seitens Microsoft) Windows Vista, Windows 7, Windows 8
- Auf einem Terminal-Server einsetzbar
- Bildschirm mit einer Auflösung von min. 1024x768
- Grafikkarte mit 16bit Farbtiefe (min. 256 Farben)
- LAN-Interface
- Standard Maus und Tastatur
- Internetzugang für Support bzw. Updates

16.3.2 BLF-Server

Der BLF-Server verteilt Besetztanzeigen und Anwesenheitsstati an OpenScape Business Attendant und OpenScape Business BLF und kommt im Wesentlichen bei einer Vernetzung von OpenScape Business zum Einsatz.

Der BLF Server baut die Verbindungen zum Kommunikationssystem direkt auf. Dafür wird kein Telefon benötigt.

Der BLF-Server benötigt je Knoten eine IP User Lizenz und eine UC User Lizenz:.

- System mit UC Smart: IP User und UC Smart User Lizenz
- System mit UC Suite: IP User und UC Suite User Lizenz

Richten Sie vor dem Start des BLF-Servers zuerst die IP User Lizenz und die UC User Lizenz ein und vergeben hierfür ein entsprechendes UC Passwort.

Der BLF-Server kann bis zu 4 Knoten bedienen.

Technische Voraussetzungen

- Windows-Standard-PC oder Windows-Server
- Betriebssysteme: Windows Vista, Windows 7, Windows 8, Windows 2003 Server, Windows 2008 Server
  Empfohlen wird ein Windows-Server-Betriebssystem, da der BLF-Server im Dauerbetrieb laufen muss. (virtualisierbar auf Basis VMware Vsphere).
- Betrieb des PC mit einer festen IP-Adresse (kein DHCP)

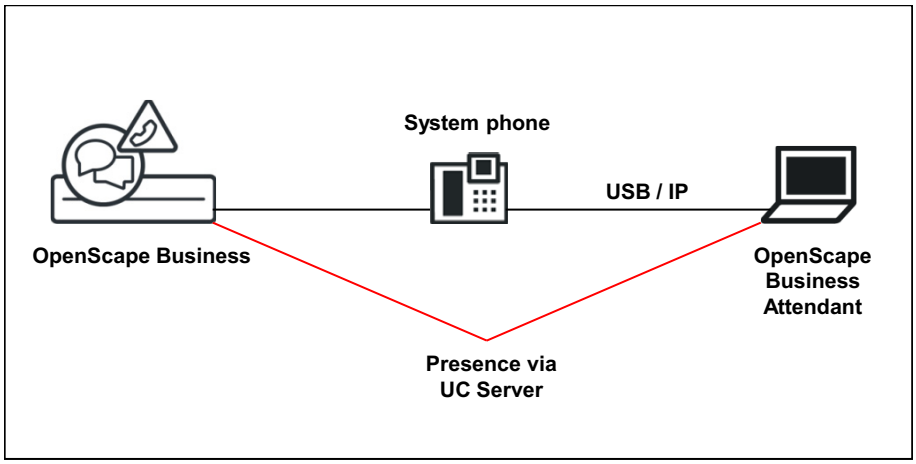
16.3.3 Einrichtebeispiele für OpenScape Business Attendant, OpenScape Business BLF und BLF-Server

In den folgenden Kapiteln finden Sie Einrichtebeispiele für die generelle Konfiguration von OpenScape Business Attendant, OpenScape Business BLF und BLF-Server.

16.3.3.1 Szenario 1: OpenScape Business Attendant an einem OpenScape Business Einzelsystem

Voraussetzungen

- Lizenz für OpenScape Business Attendant ist vorhanden
- Endgerät mit gültiger Lizenz
- Lizenz für UC Smart oder UC Suite für Presence-Information (optional)
- Die IP-Adresse für das Web Service Interface ist bei Nutzung von UC Smart oder UC Suite unterschiedlich. Im Falle von UC Smart läuft das WSI immer auf dem Kommunikationssystem, im Falle von UC Suite auf dem Application Board oder dem Application Server (siehe *UC Smart* und *UC Suite*).



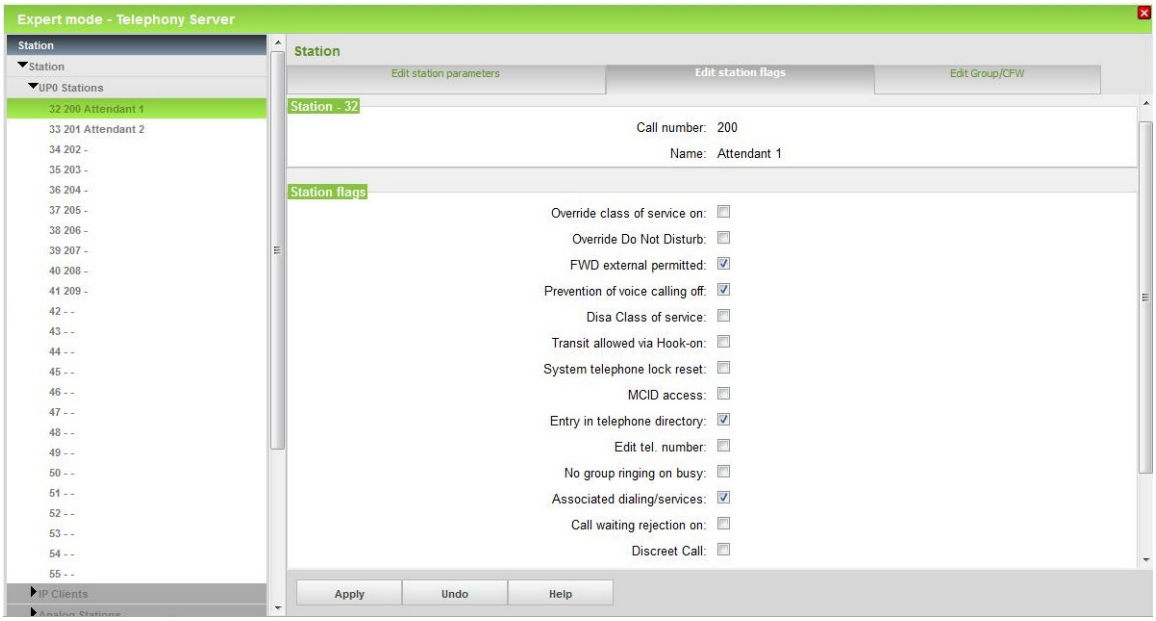
Schritt für Schritt

1) Einrichten eines Teilnehmers als Attendant über WBM oder Manager E konfigurieren (optiPoint 500, OpenStage 30T, 40T, 60T, 80T oder OpenStage 40HFA, 60HFA, 80 HFA).

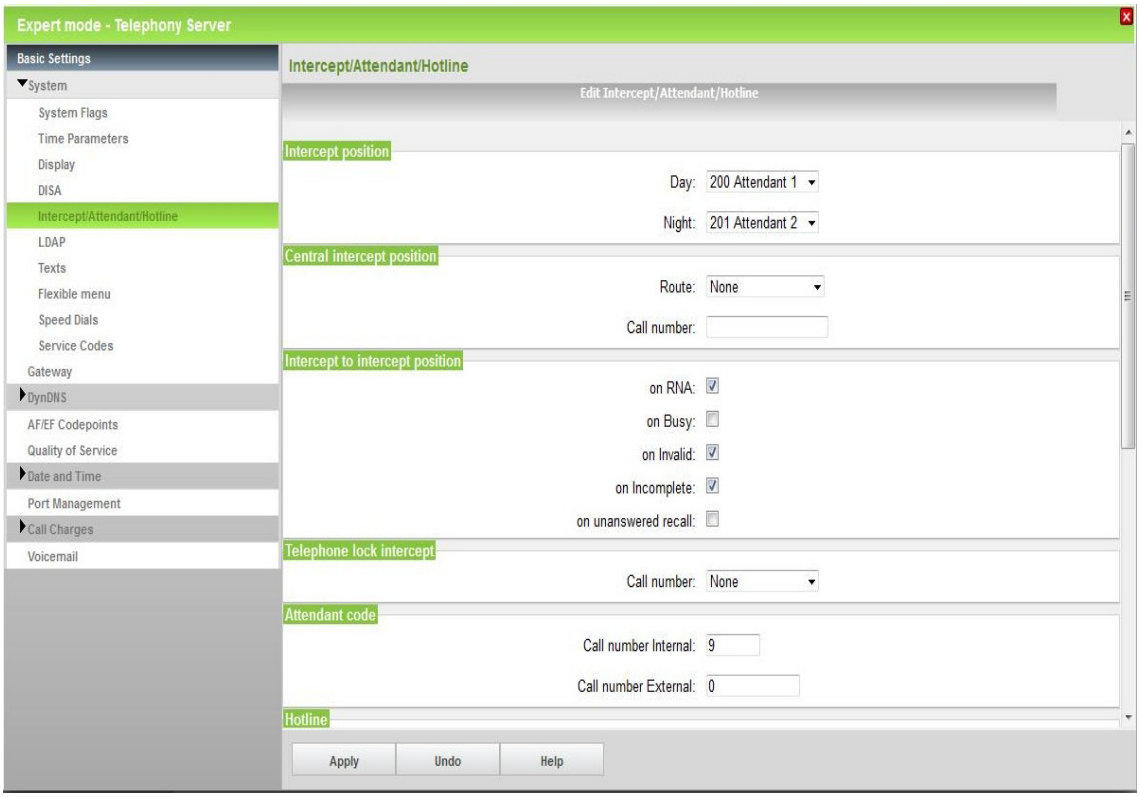
> ***INFO:*** SIP- oder CMI-Telefone sind nicht freigegeben.

2) Aktivieren Sie das Leistungsmerkmal **Assoziierte Dienste**. Dies ist erforderlich für den OpenScape Business Attendant zum Aktivieren und Deaktivieren von Leistungsmerkmalen für andere Teilnehmer.

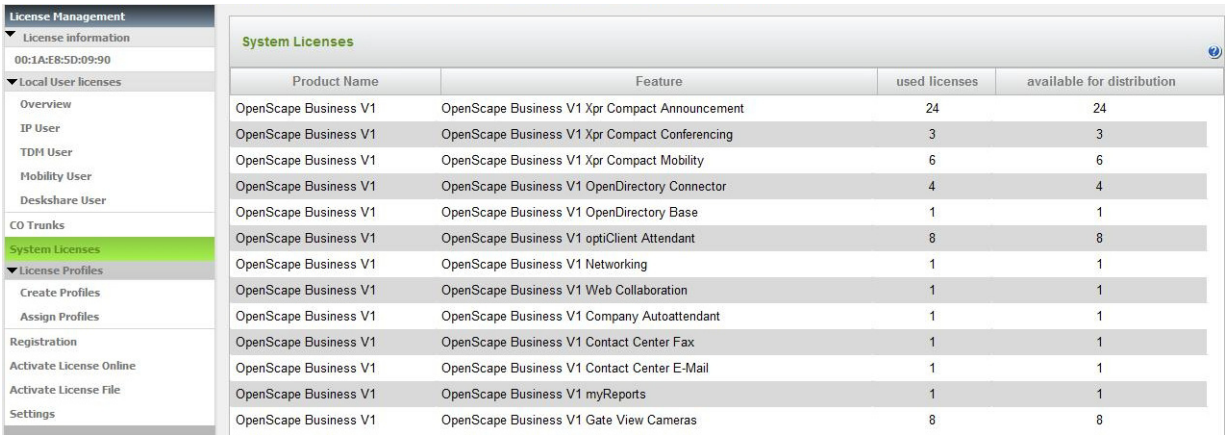
3) Aktivieren Sie **Anrufschutz durchbrechen** und deaktivieren Sie den **Anklopfschutz**.



4) Konfigurieren Sie die Abwurfkriterien und Platzkennzahlen (Definieren der Abwurfoptionen und der Rufnummern für den Vermittlungsplatz).

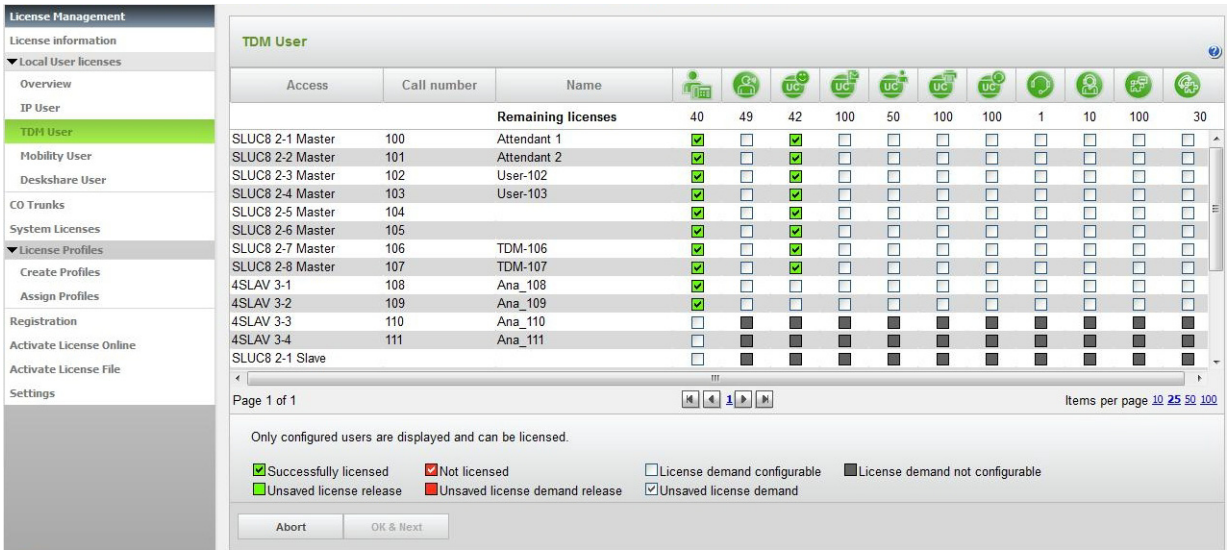


5) Lizenzierung des OpenScape Business Attendant

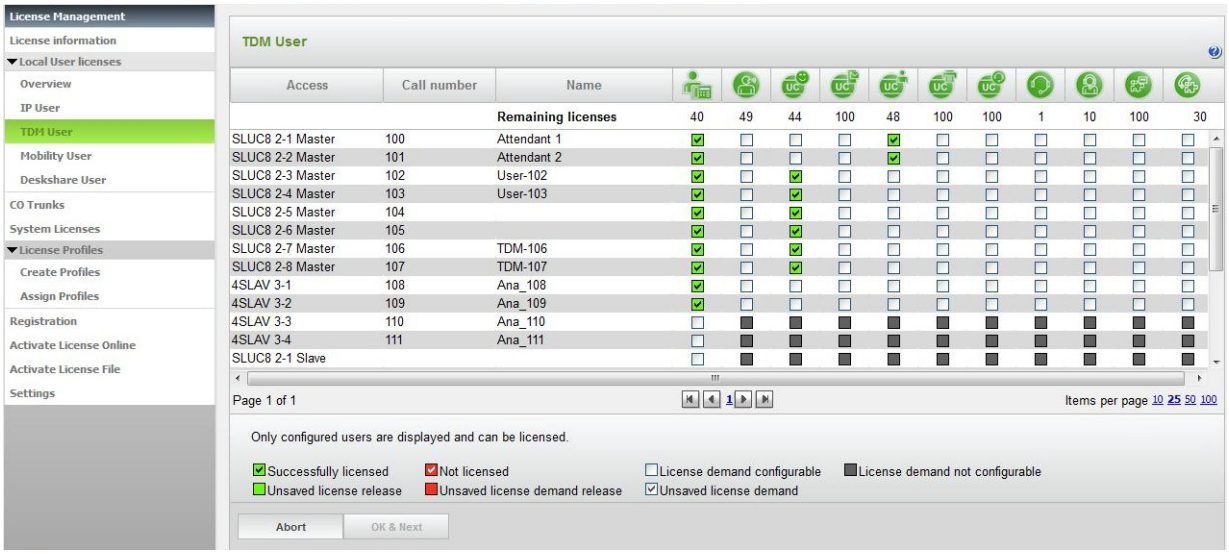


Product Name	Feature	used licenses	available for distribution
OpenScape Business V1	OpenScape Business V1 Xpr Compact Announcement	24	24
OpenScape Business V1	OpenScape Business V1 Xpr Compact Conferencing	3	3
OpenScape Business V1	OpenScape Business V1 Xpr Compact Mobility	6	6
OpenScape Business V1	OpenScape Business V1 OpenDirectory Connector	4	4
OpenScape Business V1	OpenScape Business V1 OpenDirectory Base	1	1
OpenScape Business V1	OpenScape Business V1 optiClient Attendant	8	8
OpenScape Business V1	OpenScape Business V1 Networking	1	1
OpenScape Business V1	OpenScape Business V1 Web Collaboration	1	1
OpenScape Business V1	OpenScape Business V1 Company Autoattendant	1	1
OpenScape Business V1	OpenScape Business V1 Contact Center Fax	1	1
OpenScape Business V1	OpenScape Business V1 Contact Center E-Mail	1	1
OpenScape Business V1	OpenScape Business V1 myReports	1	1
OpenScape Business V1	OpenScape Business V1 Gate View Cameras	8	8

6) Lizenzierung des Presence- bzw. Anwesenheitsstatus (UC Smart)



7) Oder: Lizenzierung des Presence- bzw. Anwesenheitsstatus (UC Suite)



8) Optional: Bei Einrichtung eines Attendants als IP-Teilnehmer muss am Telefon ein Passwort für den Benutzerzugang eingerichtet werden.

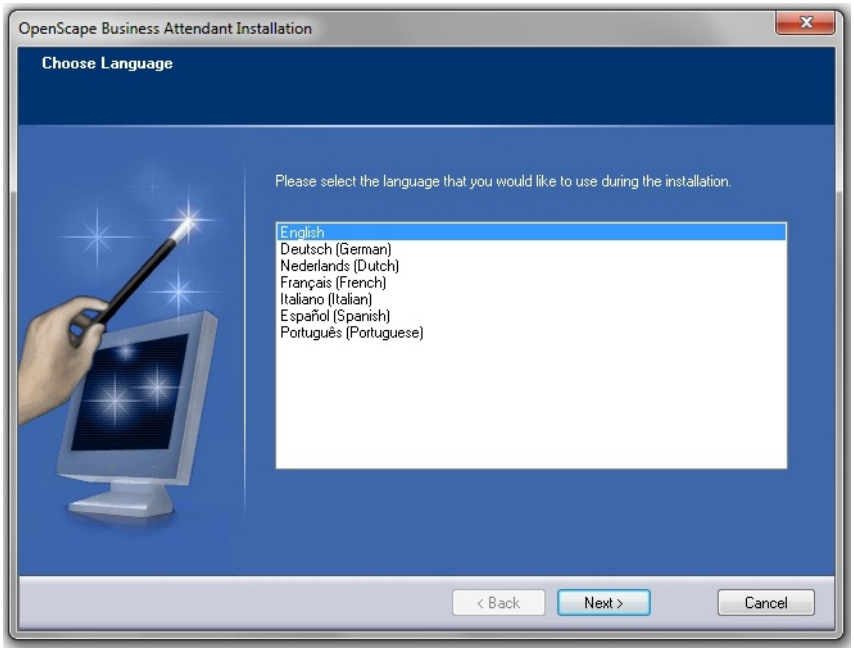


9) USB-Treiber installieren

USB - COM Treiber (Callbridge) für optiPoint 500, OpenStage30T und OpenStage 40T

USB - RNDIS Treiber für OpenStage 60T und OpenStage 80T

10) OpenScape Business Attendant über die Installationsroutine installieren (Lizenzvereinbarung zustimmen, Angabe des Speicherorts und der Sprache desOpenScape Business Attendants).

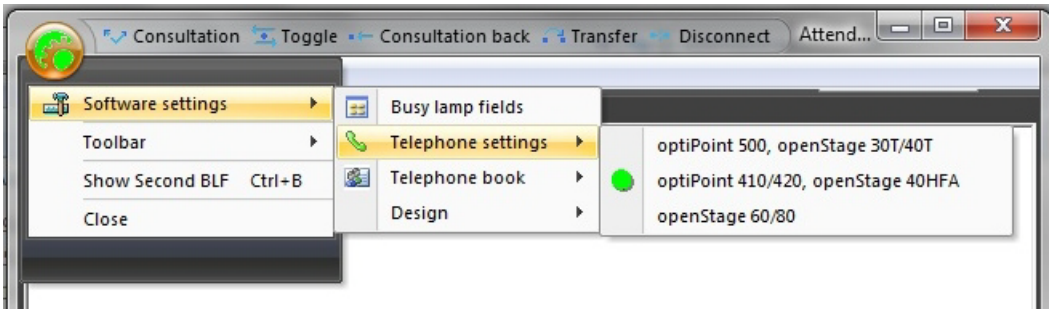


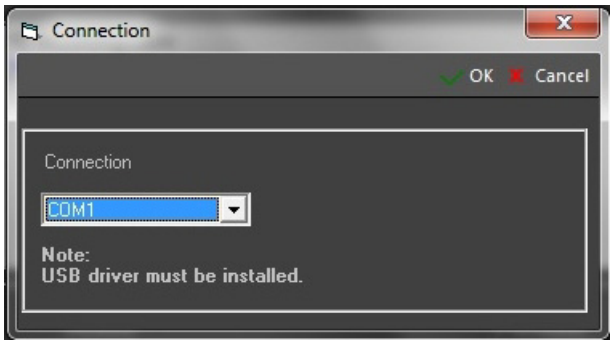
Nach der Installation und dem erstem Start des Programms wird automatisch der Einrichteassistent gestartet, der folgende Einstellungen abfragt:

Art des Telefons

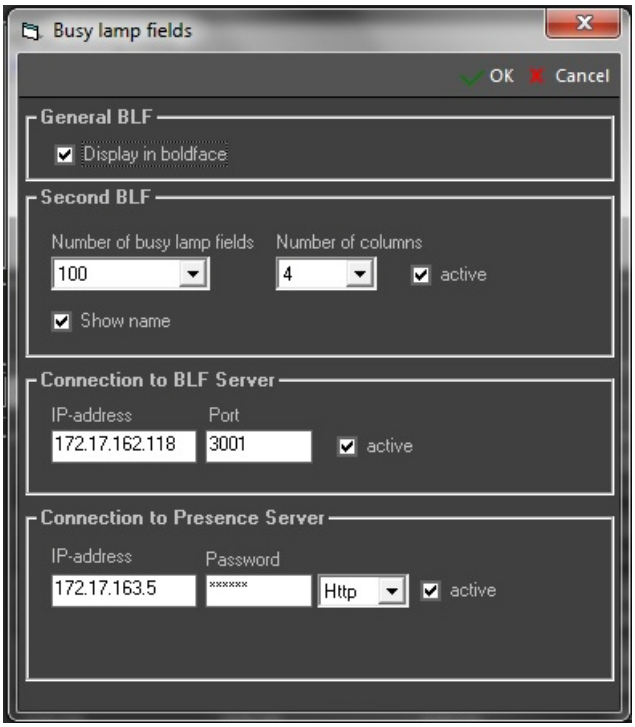
Soll die Presence-Funktion genutzt werden

Konfiguration für den Zugang im Attendant:

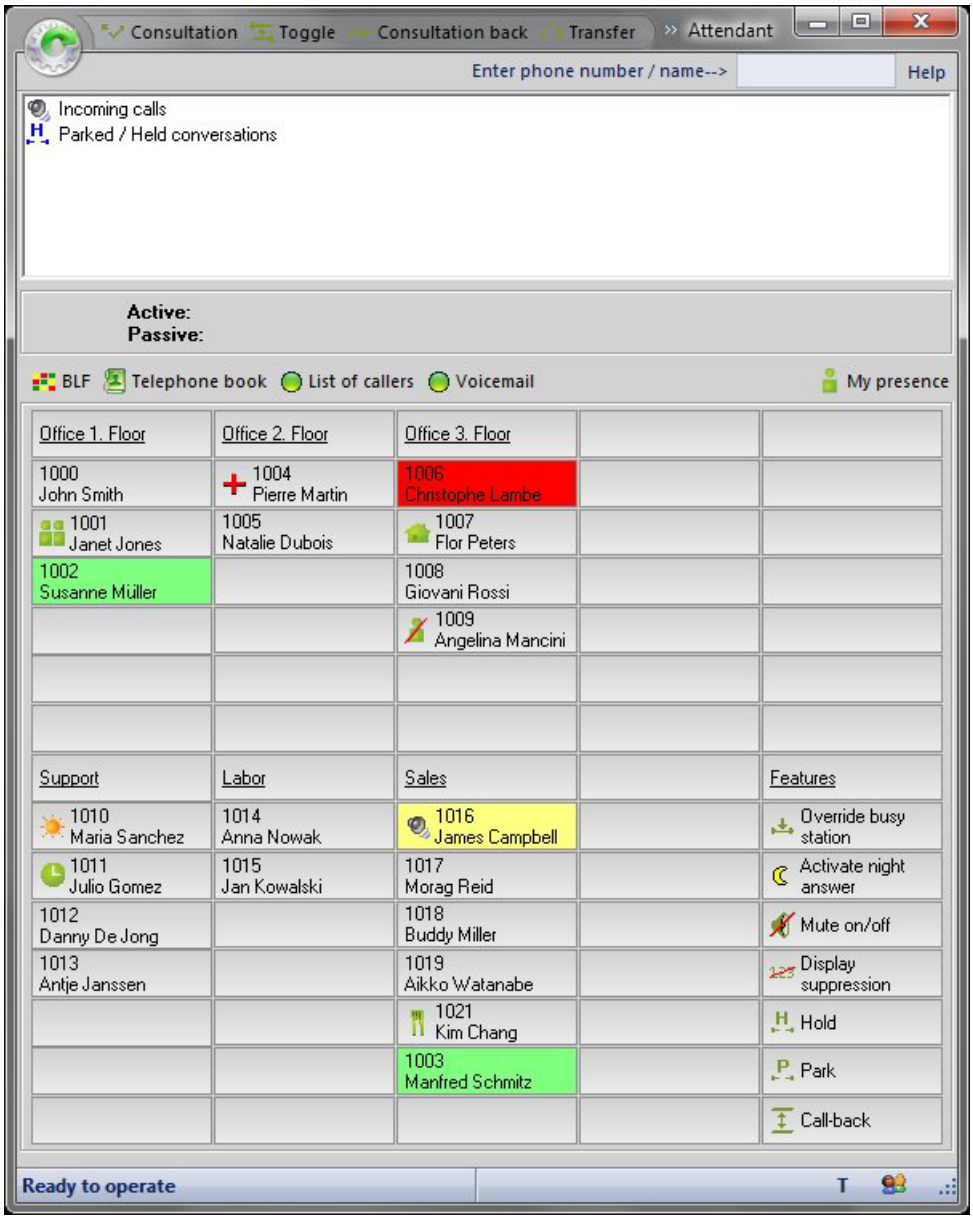




Nach erfolgreicher Anmeldung am Kommunikationssystem besteht die Möglichkeit das BLF automatisch zu füllen (Anzahl der gewünschen BLF Felder und Zurgangsparameter für BLF-Server (optional) und Presence Server).



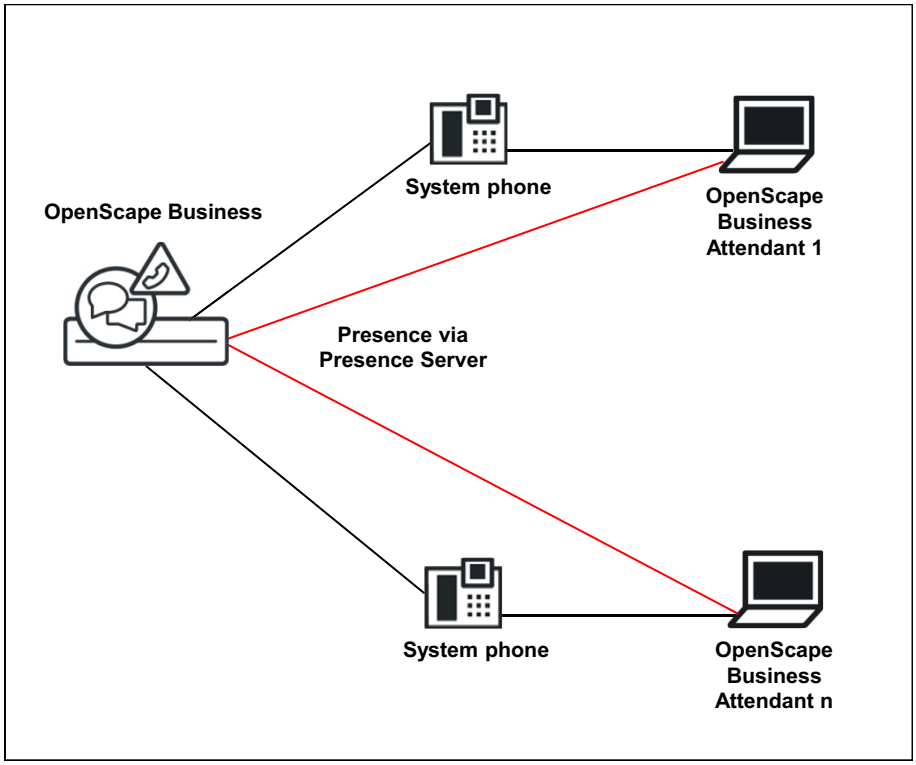
INFO: Sicherheitseinstellungen (http oder https) im WBM vergeben bzw. prüfen.


Consultation
Toggle
Consultation back
Transfer
Attendant
Enter phone number / name-->
Help
Incoming calls
Parked / Held conversations
Active:
Passive:
BLF
Telephone book
List of callers
Voicemail
My presence
Office 1. Floor
Office 2. Floor
Office 3. Floor
1000 John Smith
1004 Pierre Martin
1006 Christophe Lambe
1001 Janet Jones
1005 Natalie Dubois
1007 Flor Peters
1002 Susanne Müller
1008 Giovani Rossi
1009 Angelina Mancini
Support
Labor
Sales
Features
1010 Maria Sanchez
1014 Anna Nowak
1016 James Campbell
Override busy station
1011 Julio Gomez
1015 Jan Kowalski
1017 Morag Reid
Activate night answer
1012 Danny De Jong
1018 Buddy Miller
Mute on/off
1013 Antje Janssen
1019 Aikko Watanabe
Display suppression
1021 Kim Chang
Hold
1003 Manfred Schmitz
Park
Call-back
Ready to operate

16.3.3.2 Szenario 2: Zwei oder mehrere OpenScape Business Attendant an einem OpenScape Business Einzelsystem

Voraussetzungen

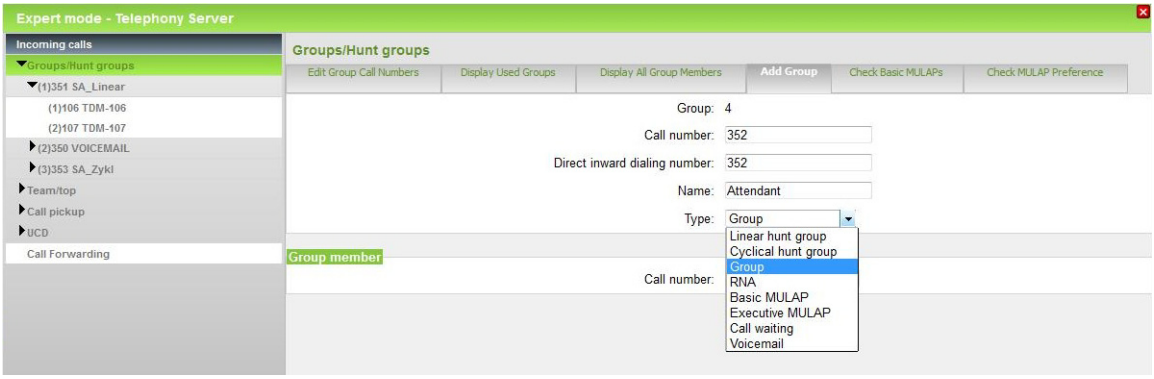
- Additiv zum Szenario 1 sind folgende Voraussetzungen erforderlich:
- Ausreichende Lizenzen für UC Smart oder UC Suite für Presence-Information (optional)
- Gruppenkonfiguration
- Text bei Parken nur bei vorhandenem BLF-Server



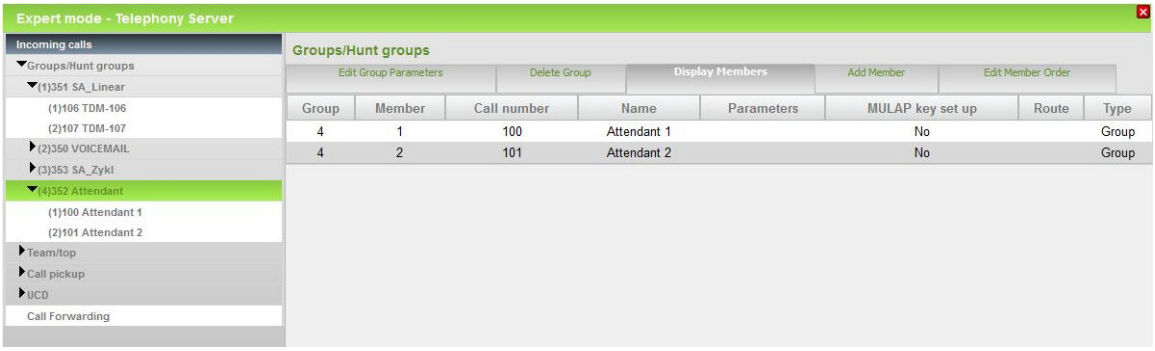
Schritt für Schritt

1) Einrichten eines Teilnehmers als Attendant über WBM (siehe Einrichtebeispiel 1).

2) Definieren einer Gruppe, dabei werden Sammelanschluß (linear und zyklisch) und Rufgruppen unterstützt.



3) Zuweisen der Attendants (der entsprechenden Teilnehmer) zur Gruppe.



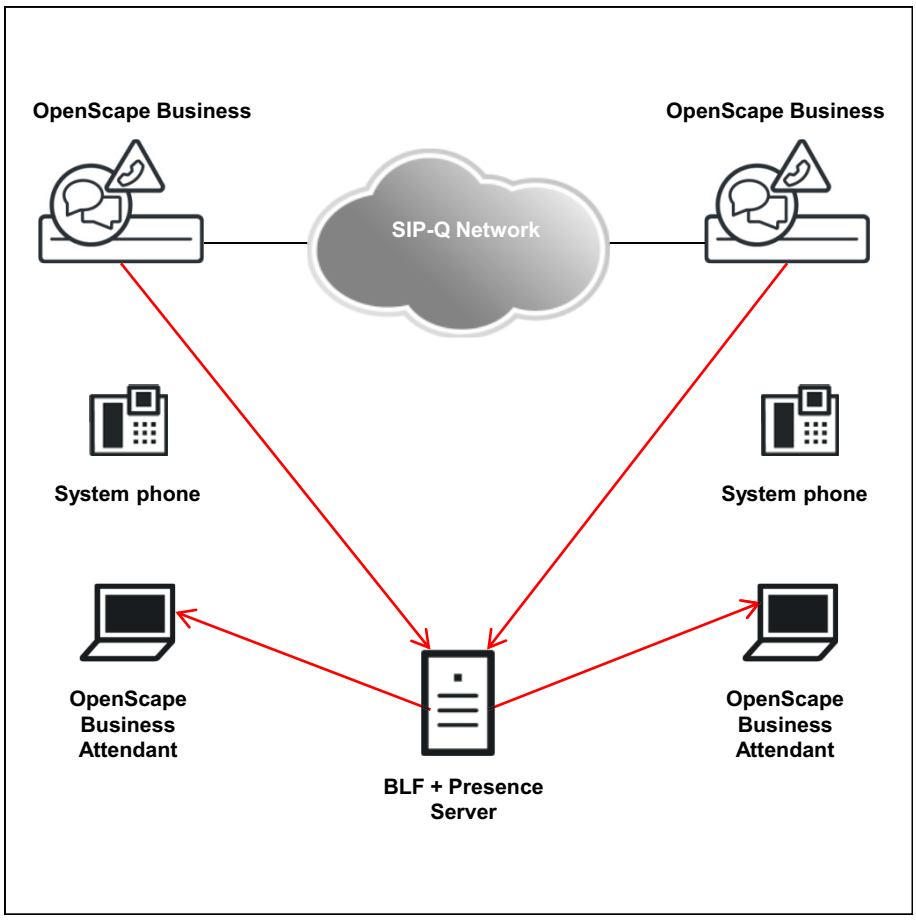
INFO: Konfigurieren Sie die Abwurfkriterien und Platzkennzahlen (Definieren der Abwurfoptionen und der Rufnummern für den Vermittlungsplatz). Der Abwurfplatz ist in diesen Fällen die Gruppen-Rufnummer.

INFO: Bei Betrieb von mehreren Attendants in einem Kommunikationssystem besteht die Möglichkeit, Zusatztexte für geparkte Gespräche an allen Attendants anzuzeigen. Hierzu ist zwingend die Installation eines BLF-Servers erforderlich.

16.3.3.3 Szenario 3: OpenScape Business Vernetzung mit jeweils eigenen OpenScape Business Attendants (netzweite BLF und Anwesenheitsstatus über BLF-Server)

Voraussetzungen

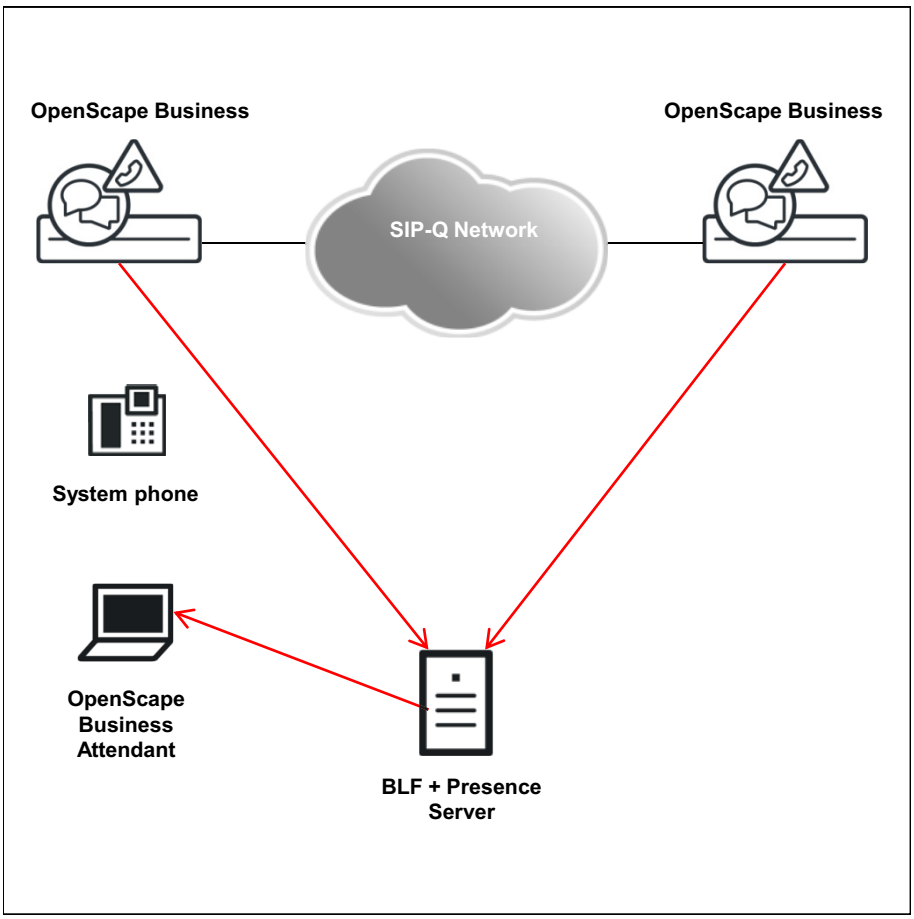
- Lizenz für UC Smart oder UC Suite für Presence-Information (optional)
- Eingerichteter BLF-Server (siehe Szenario 7)



16.3.3.4 Szenario 4: OpenScape Business Vernetzung mit zentralem OpenScape Business Attendant (netzweite BLF und Anwesenheitsstatus über BLF-Server)

Voraussetzungen

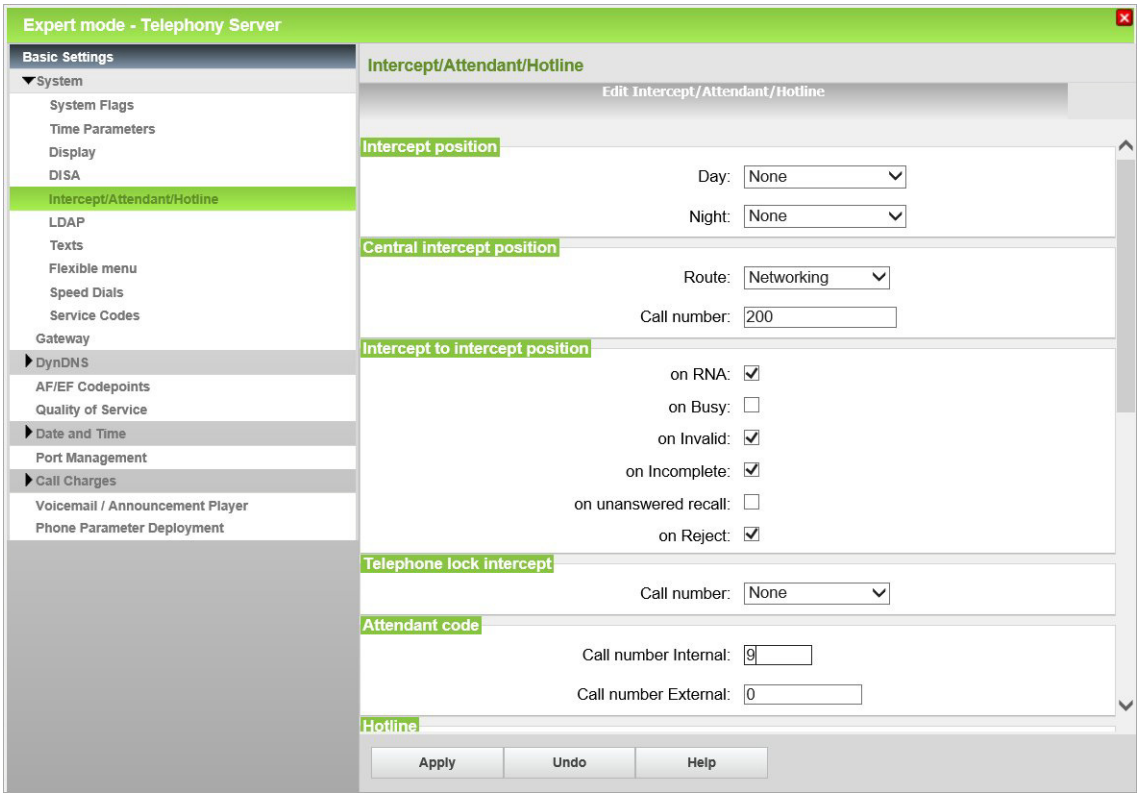
- Lizenz für UC Smart oder UC Suite für Presence-Information (optional)
- Eingerichteter BLF Server (siehe Scenario 7)
- Zentraler Abwurfplatz (in dem Knoten, in dem kein OpenScape Business Attendant eingerichtet ist)



Schritt für Schritt

1) Einrichten des OpenScape Business Attendant gemäß Einrichtebeispiel 1.

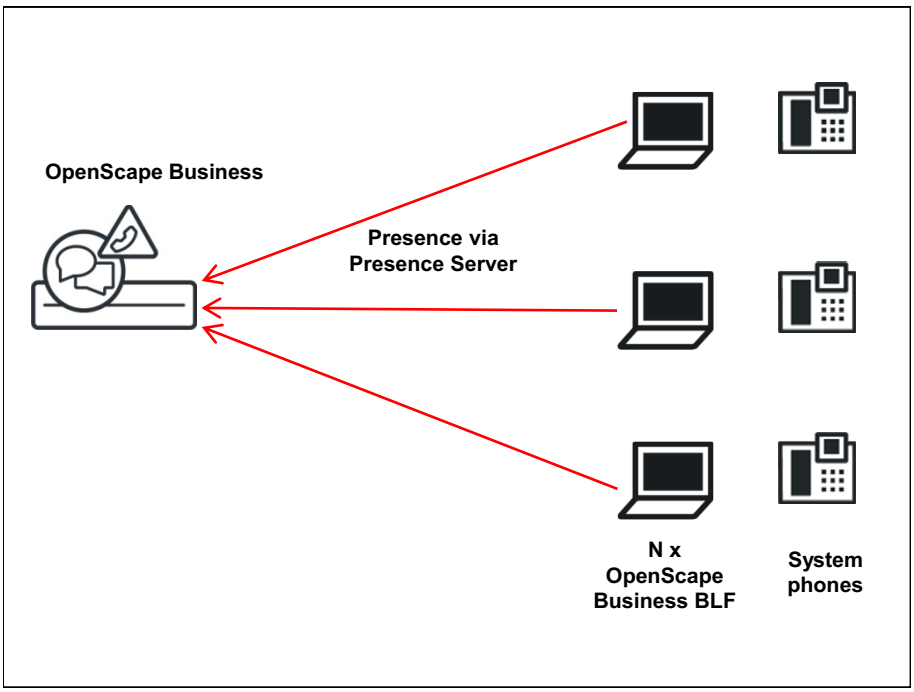
2) In dem Knoten (in dem kein OpenScape Business Attendant eingerichtet ist) den zentralen Abwurfplatz eintragen.



16.3.3.5 Szenario 5: OpenScape Business BLF an einem OpenScape Business Einzelsystem

Voraussetzungen

- Eine OpenScape Business BLF Lizenz je Teilnehmer ist vorhanden
- Telefone sind bereits zugeordnet
- Eine UC-Smart oder UC-Suite-Lizenz je Teilnehmer ist vorhanden



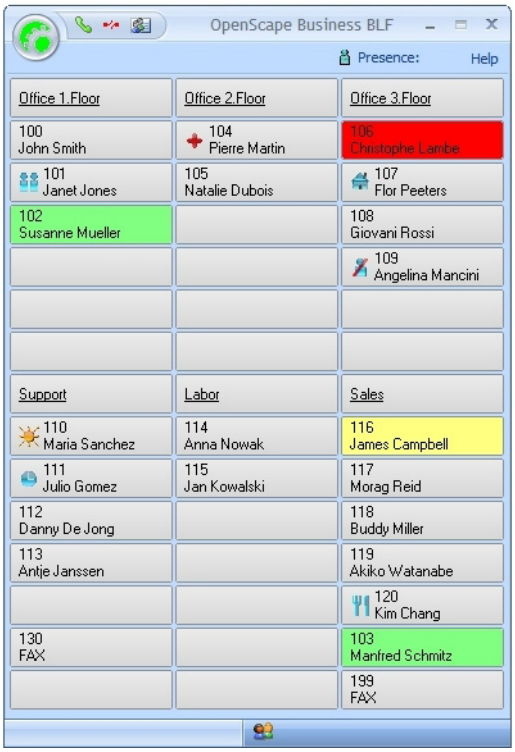
Schritt für Schritt

1) Telefone über WBM einrichten

2) Presence Server über WBM einrichten

3) OpenScape Business BLF installieren und starten

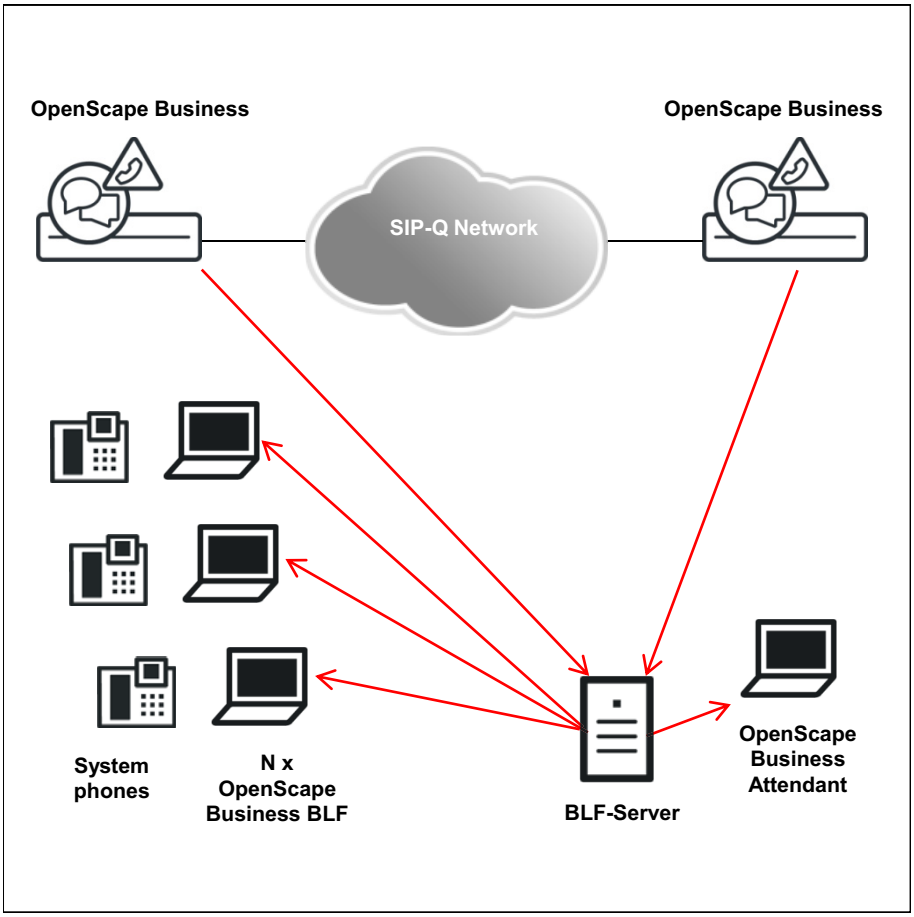
4) Nach dem ersten Hochlauf erfolgtdie Anbindung an den BLF-Server sowie die (optional) automatische Belegung des OpenScape Business BLF.



16.3.3.6 Szenario 6: OpenScape Business BLF an einem OpenScape Business Netzverbund (BLF und Anwesenheitsstatus über BLF-Server)

Voraussetzungen

- Eine OpenScape Business-BLF-Lizenz je Teilnehmer ist vorhanden
- Telefone sind bereits zugeordnet
- Eine UC-Smart- oder UC-Suite-Lizenz je Teilnehmer ist vorhanden
- BLF-Server einrichten (siehe Szenario 7)



Schritt für Schritt

1) Telefone über WBM einrichten
2) Presence Server über WBM einrichten
3) OpenScape Business BLF installieren und starten
4) Nach dem ersten Hochlauf erfolgt die Anbindung an den BLF-Server sowie die manuelle Belegung des BLF. In diesem Fall kann das BLF mit netzweiten Teilnehmern belegt werden.

16.3.3.7 Szenario 7: BLF-Server einrichten

Voraussetzungen

- Die OpenScape Business Attendant CD mit dem BLF-Server-Installationsprogramm `BLF Server.exe` ist vorhanden.
- Es wird kein Telefon benötigt. Der BLF-Server baut die Verbindungen zum Kommunikationssystem direkt auf.
- Der BLF Server benötigt pro Knoten eine IP User Lizenz und eine UC Smart User Lizenz (mit UC-Lösung UC Smart) oder eine UC Suite User Lizenz (mit

UC-Lösung UC Suite). Richten Sie bitte vor dem Start die Lizenzen ein und vergeben ein UC Kennwort.

- Eventuell muss für den BLF-Server der Port 3001 (default) in der Firewall geöffnet werden.

Schritt für Schritt

1) BLF-Server installieren:

a) Starten Sie das BLF-Server-Installationsprogramm `BLF Server.exe`.

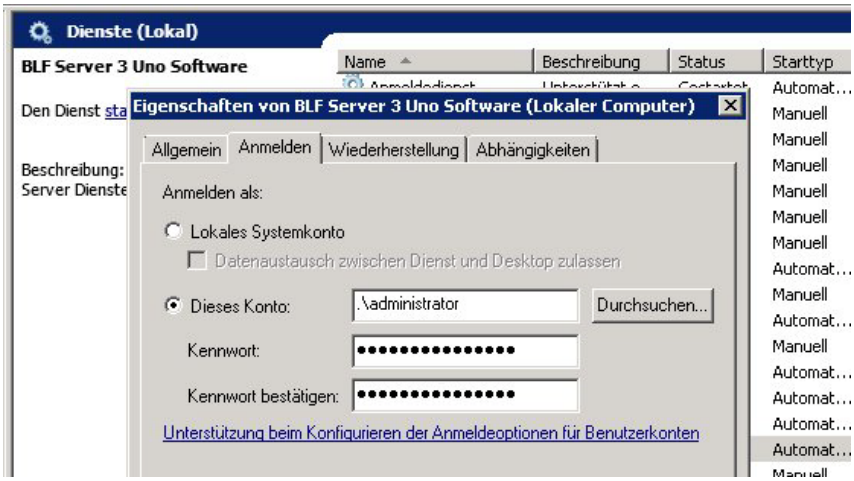
b) Folgen Sie den Anweisungen des Installationsprogramms.

2) Benutzer-Konto des BLF-Server-Dienstes ändern:

a) Schließen Sie den BLF-Server, falls geöffnet.

b) Öffnen Sie die Diensteverwaltung (z. B. über **Systemsteuerung > Verwaltung > Dienste**) und klicken Sie bei dem Dienst **BLF Server 3 Uno Software** mit der rechten Maustaste auf **Eigenschaften**.

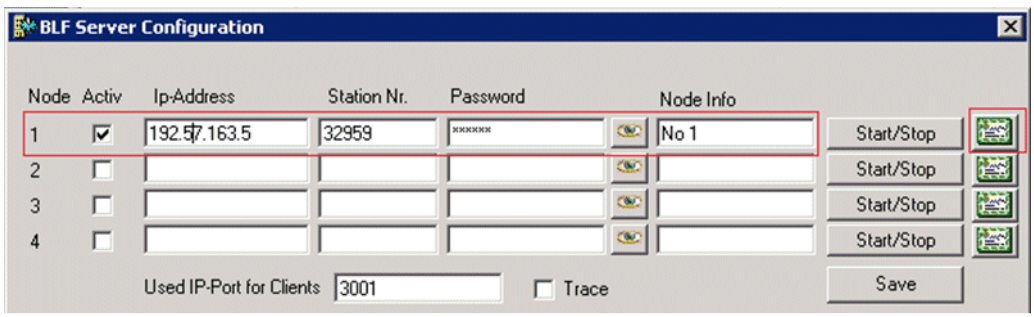
c) Wechseln Sie vom lokalen Systemkonto auf das Administratorkonto. Geben Sie dazu das Administrator-Kennwort ein.



3) BLF-Server konfigurieren:

a) Starten Sie den BLF-Server. Es erscheint das Fenster **BLF Server Status** und ein weiteres Fenster mit Konfigurationshinweisen.

b) Klicken Sie im Fenster **BLF Server Status** auf **Datei > Konfiguration**. Es öffnet sich das Fenster **BLF Server Konfiguration**.

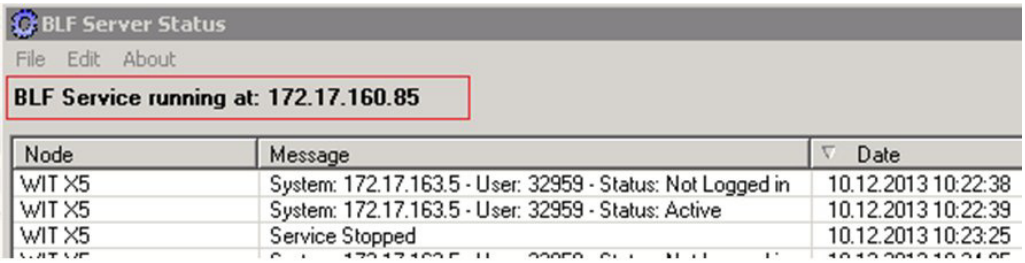


c) Geben Sie in den Feldern der ersten Zeile die Daten des ersten Knoten ein und aktivieren Sie den Knoten.

d) Klicken Sie in der Zeile des ersten Knotens auf das Symbol für die SSL-Zertifikats-Installation. Folgen Sie den Anweisungen der Zertifikats-Installation.

e) Für weitere Knoten wiederholen Sie die Schritte c) und d).

f) Klicken Sie abschließend auf **Sichern**. Sie wechseln automatisch zurück zum Fenster **BLF Server Status**. Dort werden Ihnen die laufenden Tasks angezeigt.



16.4 myAttendant

Mit myAttendant stehen Ihnen umfangreiche Vermittlungsfunktionen zur Verfügung. Die Teilnehmer werden komfortabel über Benutzerschaltflächen verwaltet. Für die Nachrichtenvermittlung (Sprach-, Fax- und Sofortnachrichten, SMS, E-Mail) steht Ihnen das Nachrichten-Center zur Verfügung.

Pro Kommunikationssystem (pro Netzknoten) können maximal 20 myAttendant angeschlossen werden. Der Maximalausbau eines Netzverbunds ist die Summe der Kapazitäten der vernetzten Kommunikationssysteme. Der Anwesenheitszustand und der Telefonstatus werden für alle Teilnehmer im Netzwerk dargestellt. Im Nachrichtencenter von myAttendant werden die Teilnehmer des eigenen Kommunikationssystems dargestellt.

Wesentliche Vermittlungsfunktionen

- Anstehende bzw. angenommene Anrufe verwalten
- Daten des aktiven Gesprächs werden angezeigt
- Geparkte, gehaltene Gespräche werden angezeigt
- Anruferliste
- Journal für offene, geplante, interne, extern, angenommene, verpasste und gehende Gespräche
- Telefonbuchanwendung
  - LDAP (z. B. ODS)
  - Persönliches telefonbuch / Outlook-Kontakte
  - Internes Verzeichnis, bei Vernetzung aller Teilnehmer im Netzwerk
- Besetztlampenfeld-Status aller internen Teilnehmer des eigenen Systems sowie aller Teilnehmer des Netzwerks

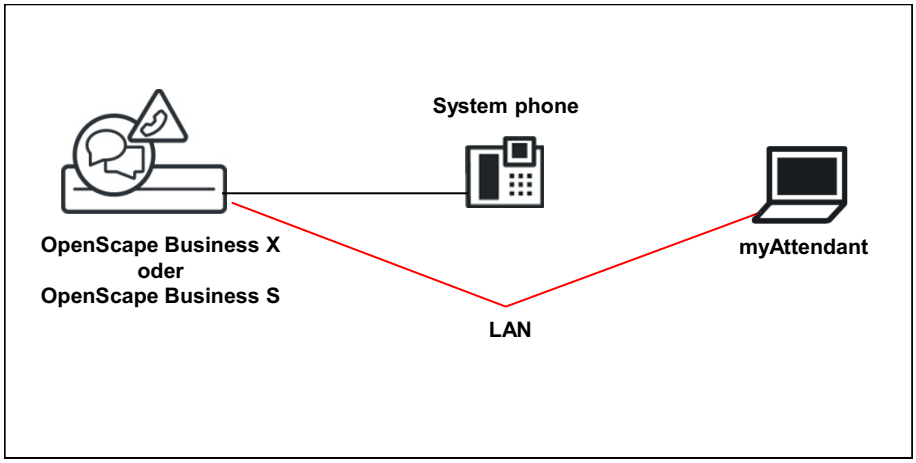
  - Telefonstatus: Frei, Besetzt, Gerufen, Umgeleitet, Anrufschutz
  - Anwesenheitsstatus: Büro, CallMe, Besprechung, Krank, Pause, Außer Haus, Urlaub, Mittagspause, Zuhause (netzweit)
- Es stehen drei Oberflächen-Styles zur Auswahl
- Es können maximal 20 myAttendant je Kommunikationssystem angeschlossen werden (max. 20 Lizenzen je OpenScape Business X3/X5/X8 und OpenScape Business S) Die Lizenzierung von myAttendant geschieht über das WBM.

Technische Voraussetzungen (Details hierzu siehe Release Notes)

- Standard Windows PC
- Betriebssysteme Windows Vista, Windows 7, Windows 8
- Terminal Server Einsatz möglich

Unterstützte Telefone

- openStage 40/60/80 HFA
- OpenScape Desk Phone IP 35G/55G HFA
- openStage 30T/40T/60T/80T
- optiPoint 500
- SIP-Telefone mit RFC 3725-Unterstützung, z. B. OpenScape Desk Phone IP 35G/55G SIP
- Einfaches Plug and Play bei der Installation, die ersten Schritte für die Installation werden dem Anwender (wenn seine Mail-Adresse konfiguriert wurde) vom System zugeschickt.



16.4.1 Teilnehmerverwaltung

Für die Verwaltung der Teilnehmer in myAttendant stehen die Benutzerschaltflächen, das interne, das externe und das persönliche Verzeichnis zur Verfügung.

Benutzerschaltflächen

Die Benutzerschaltflächen befinden sich in der Registerkarte **Standard** und sind ein Bestandteil des Hauptfensters von myAttendant.

In einer Registerkarte der Benutzerschaltflächen stehen 90 Benutzerschaltflächen zur Verfügung. Die Benutzerschaltflächen sind standardmäßig alphabetisch nach Nachname sortiert. Den Benutzerschaltflächen können interne und externe Teilnehmer zugeordnet werden.

Es können mehrere Registerkarten für Benutzerschaltflächen eingerichtet werden, die Namen für diese Benutzerschaltflächen sind frei wählbar.

16.4.2 Nachrichten-Center

Im **Nachrichten-Center** von myAttendant werden Sprach-, Fax- und Sofortnachrichten, sowie SMS und E-Mails protokolliert und verwaltet.

Nachrichten können für andere Teilnehmer verwaltet werden. Diese müssen dazu die Erlaubnis erteilt haben.

In der Teilnehmerliste sind alle Teilnehmer des Kommunikationssystems mit ihrem An-/Abwesenheitsstatus aufgelistet. An oberster Stelle steht Ihr eigener Status mit aufgeklappter Nachrichtenübersicht. Die weiteren Teilnehmer folgen in alphabetischer Reihenfolge.

Abhängig von der Auswahl in der Nachrichtenübersicht werden Nachrichtendetails angezeigt, die Informationen zu den Nachrichten werden tabellarisch angezeigt und können dort zur Bearbeitung ausgewählt werden.

Die Nachrichtentypen können wie folgt bearbeitet werden:

- **Sprachnachrichten** können abgehört, gelöscht, weitergeleitet werden,
- **LAN-Nachrichten** können gelesen, geändert und gelöscht werden,
- **Faxnachrichten** können weitergeleitet werden.

LAN-Nachrichten

LAN-Nachrichten können nur von Benutzern von myAttendant erstellt werden. Sie dienen als eine Art "Schwarzes Brett" für den Teilnehmer, auf dem er sich Notizen (zu einzelnen Teilnehmern) macht. Diese Nachrichten können angesehen, geändert oder gelöscht werden; sie können nicht an andere Teilnehmer versendet werden.

16.4.3 Szenario 1: Wie Sie myAttendant an einem OpenScape Business Einzelsystem einrichten

Voraussetzungen

- Lizenz für myAttendant ist vorhanden
- Telefon mit gültiger Lizenz
- Application Server oder Application Board vorhanden
- UC Suite ist über den Basisinstallations-Wizard aktiviert

Schritt für Schritt

1) Telefon für den Vermittlungsplatz über WBM konfigurieren

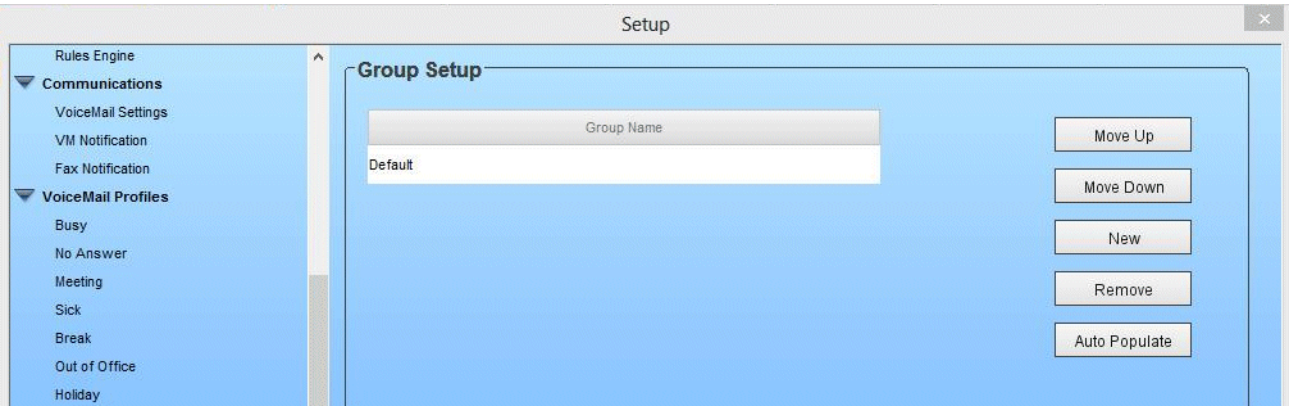
2) Deaktivieren Sie im **Experten-Modus** unter **Teilnehmer**>**IP-Clients**>**System Clients**>**Teilnehmer**>**Teilnehmer Flags ändern** den **Anklopfschutz**

3) Aktivieren sie im **Experten-Modus** unter **Telephonie**>**Grundeinstellungen**>**System >Abwurf**>**VPL**>**Hotline** das Leistungsmerkmal **Anklopfen durch VPL**.

4) Kontrollieren bzw. ändern Sie die Abwurfkriterien und Platzkennzahlen (Definieren der Abwurfoptionen und der Rufnummern für den Vermittlungsplatz).

5) Lizenzierung von myAttendant

6) Nach erfolgreicher Anmeldung am Kommunikationssystem besteht die Möglichkeit das BLF automatisch zu füllen. Dies können Sie in myAttendant in den persönlichen Einstellungen unter Gruppeneinrichtung konfigurieren.



16.4.4 Szenario 2: Wie Sie zwei oder mehrere myAttendant an einem OpenScape Business Einzelsystem einrichten

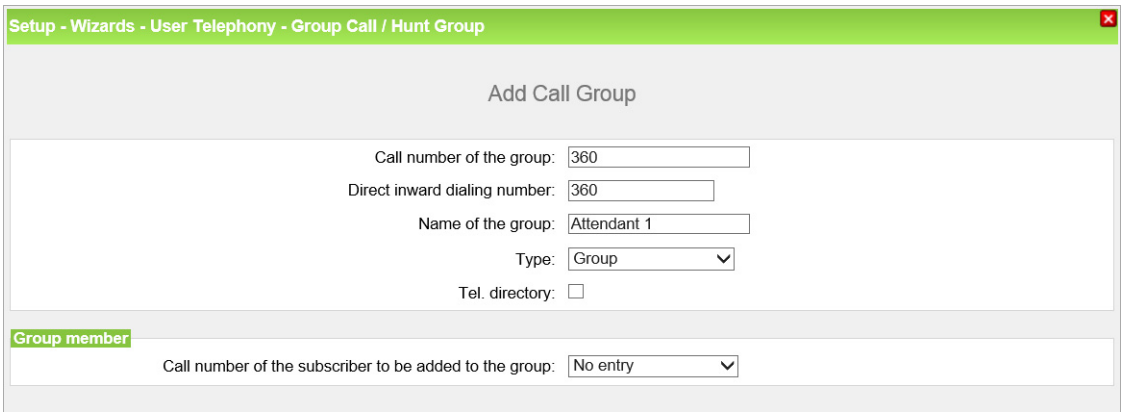
Das Szenario 2 baut auf Szenario 1 auf und wird additiv eingerichtet.

Voraussetzungen

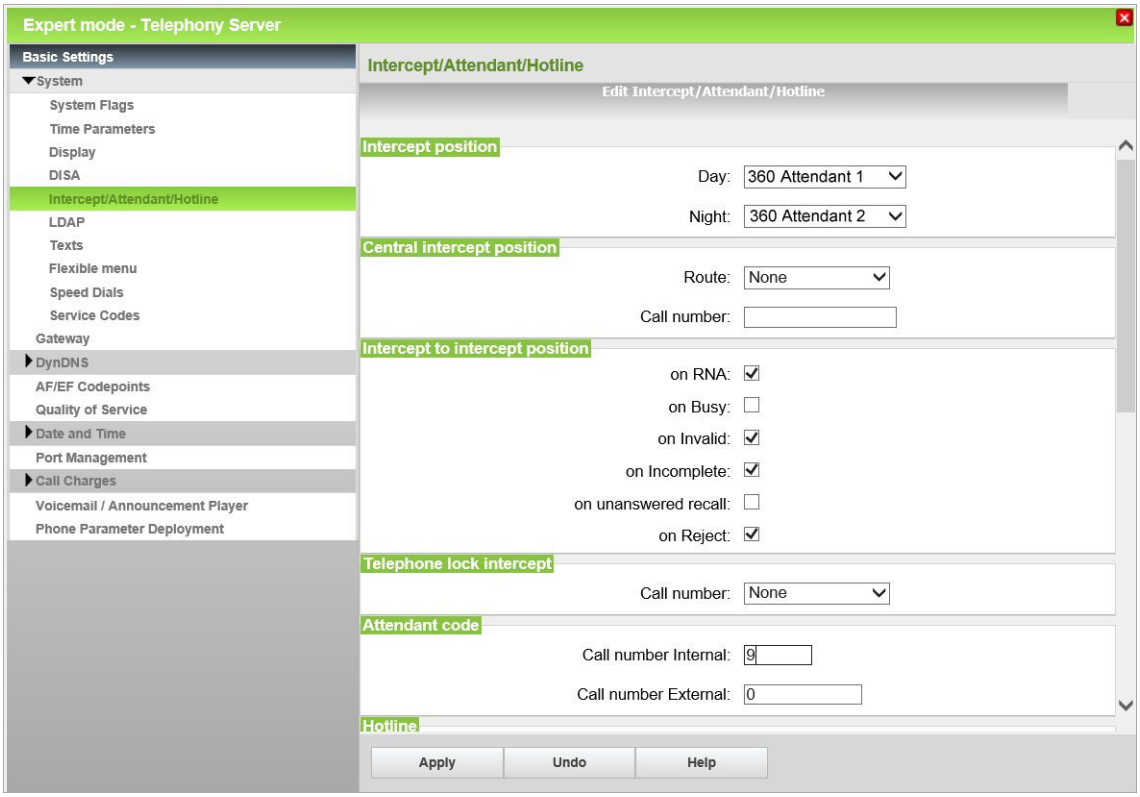
- Ausreichende Lizenzen für myAttendant
- Telefon mit gültiger Lizenz

Schritt für Schritt

1) Konfigurieren Sie eine Gruppe (die nur aus Vermittlungsplätzen besteht) im WBM unter **Einrichtung** > **User Telefonie** > **Gruppenruf**.



2) Wählen Sie diese Gruppe bei der Konfiguration der OpenStage Vermittlungsplatz Telefone aus.



16.4.5 Szenario 3: Wie Sie eine OpenScape Business Vernetzung mit zentralem myAttendant einrichten

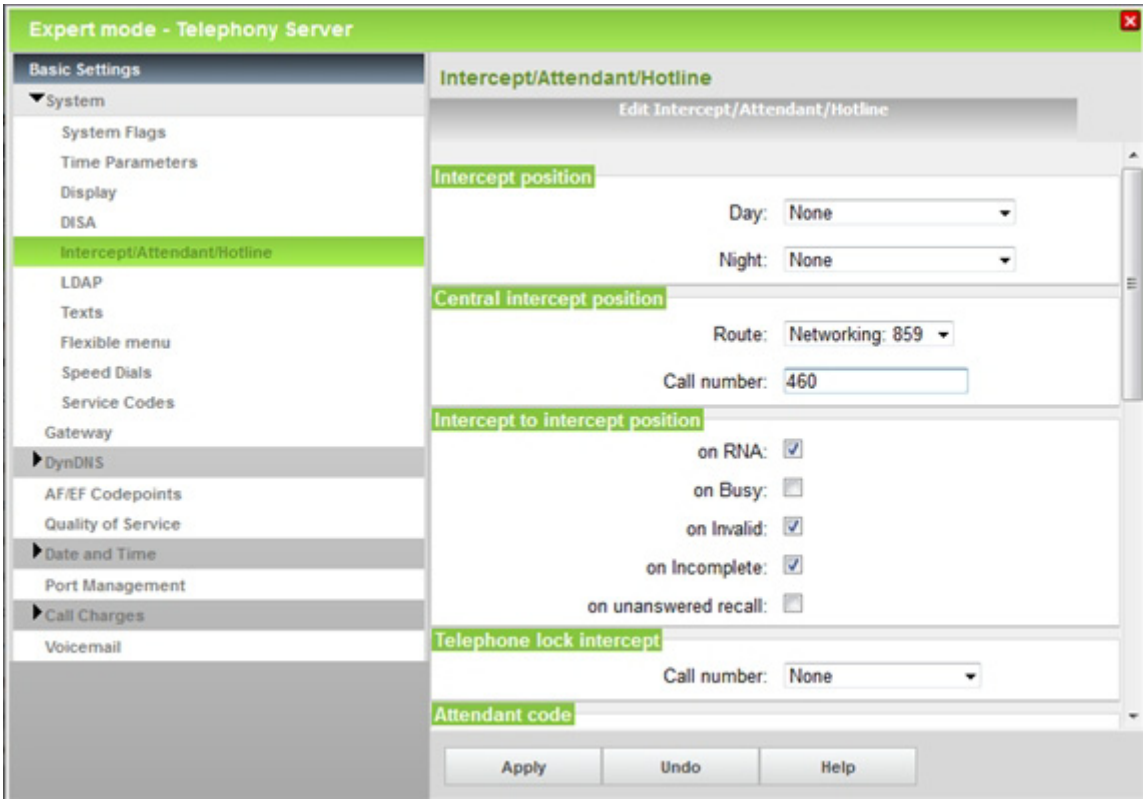
Das Szenario 3 baut auf Szenario 1 und 2 auf und wird additiv eingerichtet. Knoten 1 wird mit Knoten 2 vernetzt. Der zentrale Vermittlungsplatz ist in Knoten 2.

Voraussetzungen

- Ausreichende Lizenzen für myAttendant vorhanden
- Lizenzen für die Vernetzung sind vorhanden
- Telefon mit gültiger Lizenz
- LCR ist eingerichtet

Schritt für Schritt

1) Richten Sie einen zentralen Abwurfplatz in Knoten 1 ein. Der zentrale Abwurfplatz muss in einem Knoten angelegt sein, in dem KEIN Vermittlungsplatz eingerichtet ist.



2) Richten Sie den Vermittlungsplatzes für System 2 ein (wie in Szenario 2 beschrieben).

3) Installieren Sie myAttendant mit den Benutzerdaten von Knoten 2.

16.5 Abwurfplatz

Das Kommunikationssystem ermöglicht, externe Anrufe, die keinem Teilnehmer zuzuordnen sind oder nicht beantwortet werden, an einen festzulegenden Abwurfplatz umzuleiten, damit kein Anruf verloren geht. Die Abwurfkriterien können Sie als Administrator konfigurieren.

Der Abwurfplatz kann ein einzelner Teilnehmer, eine Gruppe oder ein Ansagegerät sein:

- Abwurfplatz (Vermittlungsplatz)
- Teilnehmer
- Sammelanschluss
- Gruppenruf
- externes Ansagegerät

Eine UCD-Gruppe darf nicht als Abwurfplatz ausgewählt werden.

Ist ein Abwurfplatz konfiguriert, werden im Abwurffall die Anrufe an diesen Abwurfplatz weitergeleitet. Ist kein Abwurfplatz konfiguriert, so werden abgeworfene Anrufe beim ersten IP-Teilnehmer signalisiert.

Ist ein interner Teilnehmer als Abwurfplatz eingerichtet, wird ihm automatisch die Standard-Tastenbelegung zugewiesen. Zusätzlich kann der Abwurfplatz für das Leistungsmerkmal "Aufschalten" berechtigt werden.

Sie können als Administrator dem Abwurfplatz für intern und extern jeweils eine Platzkennzahl (2stellig) zuweisen, unter welcher dieser direkt erreichbar ist.

Ein Abwurf wirkt systemweit, d. h. bei Gemeinschaftsanlagen für alle Teilnehmer gleich. Siehe auch "Zentraler Abwurfplatz im Netzverbund" im Kapitel Vernetzung.

Abwurfkriterien

Durch Abwurfkriterien legen Sie als Administrator fest, in welchen Situationen der Abwurf erfolgen soll. Folgende Abwurfkriterien sind möglich:

- Im Freifall
  Der Anruf folgt den Einträgen im Call Management (z. B. einer konfigurierten Rufweiterschaltung). Nimmt kein Teilnehmer den Anruf an, wird er zum Abwurfplatz weitergeleitet.
- Im Besetztfall, falls keine Weiterschaltung mehr möglich ist
  Zunächst wird geprüft, ob angeklopft werden kann. Wenn nicht angeklopft werden kann, so folgt der Anruf den Einträgen im Call Management (z. B. einer konfigurierten Rufweiterschaltung). Nimmt kein Teilnehmer den Anruf an, wird er zum Abwurfplatz weitergeleitet. Abwurf im Besetztfall bezieht sich nur auf den Erstanruf, nicht auf vermittelte oder gehende Verbindungen. Ein Wiederanruf eines externen Teilnehmers wird bei besetztem Zielteilnehmer nicht sofort abgeworfen, sondern es erfolgt Anklopfen.
- Bei Falschwahl
  Falls die gewählte Rufnummer nicht konfiguriert oder nicht aktiv ist.

- Bei unvollständiger Wahl
  Falls die gewählte Rufnummer zu kurz ist. Existiert ein zentraler Abwurfplatz, wird unvollständige Wahl nicht ausgewertet.
- Bei nicht beantwortetem Wiederanruf
  Wird ein externer Anruf nach Übergeben vor Melden nicht abgefragt und erfolgt nach Wiederanruf am ursprünglichen Ziel ebenfalls kein Melden, so erfolgt nach Ablauf der voreingestellten Zeit der Abwurf.
- Bei Ablehnung
  Falls der Anruf von einem internen Teilnehmer abgelehnt wurde, so folgt der Anruf den Einträgen im Call Management (z. B. einer konfigurierten Rufweiterschaltung). Nimmt kein Teilnehmer den Anruf an, wird er zum Abwurfplatz weitergeleitet.
- Bei fehlender Rufnummer
  Wie bei Falschwahl.
- Bei Anrufweiterschaltung mit Verkettung
  Wenn ein umgeleiteter Anruf am Ziel der Umleitung auf eine weitere Anrufumleitung trifft und dabei die Anzahl der zulässigen Verkettungen überschritten wird, erfolgt der Abwurf. Die Anzahl der zulässigen Verkettungen ist abhängig von den Eintragungen in der Rufweiterschaltung, maximal sind drei Verkettungen erlaubt.
- Bei Codeschloss
  Wählt ein Teilnehmer an einem Telefon mit aktiviertem Codeschloss eine Richtungskennzahl, erfolgt der Abwurf. Für diesen Fall legt der Administrator ein separates Abwurfziel fest.
- Bei Ansage (nur mit UC Suite)
  Wählt ein Teilnehmer die Platzkennzahl (2stellig), während er eine Ansage der Sprachbox oder des AutoAttendant hört, erfolgt der Abwurf. Für diesen Fall legt der Administrator ein separates Abwurfziel fest.

Abhängigkeiten

Thema	Abhängigkeit
Datenrufe	Datenrufe werden getrennt anstatt abgeworfen.
Sammelanschluss	Aus einem Sammelanschluss erfolgt kein Abwurf, der Ruf wird wieder zum ersten Sammelanschluss-Teilnehmer weitergeschaltet und verbleibt im Sammelanschluss.

Thema	Abhängigkeit
Standard-Tastenbelegung	Die Standard-Tastenbelegung enthält auch die Taste **Zahl der Anrufe zeigen**. Diese kann nur an 6 Endgeräte vergeben werden. Wenn die Grenze erreicht ist, werden keine Standard-Tastenbelegungen mehr vergeben. Die vergebenen Standard-Tasten werden nicht zurückgenommen, wenn ein Gerät nicht länger als Abwurfplatz definiert ist.
S_0-Leitungen	Eine Auswertung für S_0-Leitungen findet nur dann statt, wenn kein Abwurfplatz für Tag/Nacht eingerichtet ist.
Nachtschaltung	Damit bei aktivierter Nachtschaltung über DuWa- und HKZ-Leitungen jeweils das gleiche Ziel erreicht wird, muss der Eintrag für die Nachtstellen-Nummer unter Abwurf > VPL mit der **NachtRuf-Nr** in Rufzuordnung **Ltg** übereinstimmen.

16.5.1 Wie Sie Abwurfplatz und Abwurfkriterien konfigurieren

Mit dem Wizard **Vermittlungsplatz** können Sie die Rufnummern für den Abwurfplatz sowie Abwurfkriterien konfigurieren.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > User-Telefonie**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Vermittlungsplatz** zu starten.

4) Legen Sie in den Bereichen **Vermittlungsplatz** und **Platzkennzahl** (2stellig) die gewünschten Rufnummern für den Abwurfplatz fest.

5) Legen Sie im Bereich **Abwurfkriterien** die gewünschten Werte fest.

6) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

16.5.2 Wie Sie einen zentralen Abwurfplatz konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **Grundeinstellungen > System > Abwurf/ VPL/Hotline**.

4) Wählen Sie im Bereich **Zentraler Abwurfplatz** in der Aufklappliste **Richtung** den gewünschten Eintrag.

5) Geben Sie im Bereich **Zentraler Abwurfplatz** die gewünschte **Rufnummer** für **Tag** und **Nacht** ein.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

16.5.3 Wie Sie Abwurf bei Codeschloss konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **Grundeinstellungen > System > Abwurf/ VPL/Hotline**.

4) Wählen Sie im Bereich **Abwurf bei Codeschloss** in der Aufklappliste **Rufnummer** den gewünschten Eintrag.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

16.5.4 Wie Sie Abwurf bei Ansage konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Applikationen > UC Suite**.

3) Klicken Sie im Menübaum auf **Server**.

4) Klicken Sie auf die Registerkarte **Allgemeine Einstellungen**.

5) Geben Sie im Bereich **Rufnummer des Abwurfplatzes** im Feld **Zielnummer** die Rufnummer für den Abwurfplatz ein.

6) Klicken Sie auf **Speichern** und schließen Sie das Fenster.

17 Multimedia Contact Center

Das Contact Center ist eine leistungsstarke Lösung zur optimalen Verteilung und Bearbeitung von kommenden Anrufen, Faxen und E-Mails. Die intelligente, fähigkeitsbasierte Verteilung stellt sicher, dass Anrufer unabhängig vom Kontaktmedium mit dem am besten qualifizierten Contact-Center-Agenten verbunden werden. Über die Applikation myAgent stehen den Contact-Center-Agenten komfortable Funktionen für die Bearbeitung und Nachbearbeitung von Anrufen, Faxen und E-Mails zur Verfügung. myReports stellt für die Auswertung des Contact-Center-Betriebs vielfältige Berichtsvorlagen zur Verfügung.

Das Multimedia Contact Center ist vollständig in die UC-Suite-Software integriert. Alle benötigten Software-Komponenten sind enthalten. Die Contact-Center-Funktionen selbst werden über Lizenzen freigeschaltet.

Das Contact Center nutzt die Ressourcen des Kommunikationssystems, wie zum Beispiel Warteschlangen für kommende Anrufe und Unified-Communications-Funktionen für die Aufnahme und die Wiedergabe von Ansagen.

Die zentrale Software-Komponente des Contact Centers steuert alle Routing-Funktionen für kommende Anrufe, Faxe, E-Mails und steuert die über LAN angeschlossenen PC-Arbeitsplätze der Agenten und Wandanzeigen.

Auf den PC-Arbeitsplätzen der Agenten wird die Applikation myAgent installiert. Optional kann auch die Applikation myReports zur Generierung und Versendung von Berichten installiert werden. Die erforderliche Software kann direkt aus dem Downloadbereich des Kommunikationssystems heruntergeladen und auf den Client-PC installiert werden.

Mittels WBM wird die Einrichtung der Contact-Center-Grundfunktionen, der Zeitpläne und Verteilregeln sowie der Agenten vorgenommen. Einstellungen für den täglichen Betrieb des Contact Centers, wie zum Beispiel die Zuordnung von Agenten zu Warteschlangen können auch direkt über myAgent getätigt werden.

Steht das Contact Center aufgrund von Problemen (Absturz, fehlende Verbindung oder ähnliches) nicht zur Verfügung, kann eine Rückfalllösung über die UCD-Funktion des Kommunikationssystems realisiert werden. Verteilregeln für den Notfall müssen bei der Einrichtung der UCD-Gruppen im Rahmen der Ersteinrichtung des Contact Centers berücksichtigt werden.

> ***INFO:*** Informationen zur UC Suite und den Unified-Communications-Funktionen können dem Kapitel UC Suite entnommen werden.

17.1 Contact Center Clients

Die Applikation myAgent stellt den Contact Center-Agenten komfortable Funktionen für die Bearbeitung und Nachbearbeitung von Anrufen, Faxen und E-Mails zur Verfügung. Über die Applikation myReports können Berichte (Reports) über Anrufe, Warteschlangen, Agenten, Performance, Servicelevel und Nachbe-

arbeitungscodes des Contact Centers erstellt werden. Mehr als 100 vordefinierte Berichtsvorlagen stehen zur Verfügung. Darüber hinaus können eigene Berichtsvorlagen definiert werden.

17.1.1 myAgent

Allen Agenten stehen über myAgent komfortable Funktionen für die Bearbeitung und Nachbearbeitung von Anrufen, Faxen und E-Mails zur Verfügung.

myAgent bietet folgende Leistungsmerkmale:

- Bearbeitung von
  - Anrufen
  - Faxen
  - E-Mails
- Rückruffunktion für Agenten
- Anzeige und Änderung des Agentenstatus
- Anzeige und Änderung des Anwesenheitsstatus interner Teilnehmer des Kommunikationssystems
- Darstellung der Warteschlangen in Echtzeit
- Aufzeichnung von Anrufen, sofern im Kommunikationssystem aktiviert
- Anforderung um Unterstützung durch
  - Mithören von Anrufen (länderabhängig)
  - Aufschalten auf Anrufe
  - Instant Messaging
- Einbindung des internen Verzeichnisses, des externen Verzeichnisses und des externen Offline-Verzeichnisses (LDAP) für die Suche nach Namen
- Erstellung von Berichten auf Basis vordefinierter Berichtsvorlagen

In Abhängigkeit vom zugewiesenen Berechtigungs-Level stehen einem Agenten Standardfunktionen (Agent) oder erweiterte Funktionen (Supervisor oder Administrator) in myAgent zur Verfügung (siehe *Administratordokumentation, Multimedia Contact Center*).

Die Zuordnung von Agenten zu Warteschlangen erfolgt mit Hilfe der Applikation myAgent. Diese Zuordnung kann ein Agent mit dem Berechtigungs-Level Supervisor oder Administrator durchführen. Dabei können den Agenten folgende Eigenschaften zugewiesen werden (Agentenzuweisung), die Einfluss auf die Verteilung der Anrufe, Faxe und E-Mails in einer Warteschlange haben:

- **Hauptagent** oder **Agent bei Überlauf**
  An Hauptagenten werden Anrufe gleichmäßig verteilt. Ein Agent bei Überlauf erhält einen Anruf nur dann, wenn die Anrufe eine bestimmte Anzahl überschritten haben oder ein Anruf eine bestimmte Wartezeit überschritten hat.

- **Überlauf nach Sekunden**
  Anrufe, die diese Wartezeit überschreiten, erhält ein Agent bei Überlauf.
- **Überlauf nach Anrufen**
  Anrufe, die über diese Maximalzahl hinausgehen, erhält ein Agent bei Überlauf.
- **Fähigkeits-Level**
  Das Fähigkeits-Level steuert die Verteilung der Anrufe auf die Agenten in einer Warteschlange: Agenten mit höherem Fähigkeits-Level werden bei der Anrufverteilung bevorzugt. Haben alle Agenten den gleichen Fähigkeits-Level, erhält der am längsten freie Agent den Anruf.
- **Agentenrückruf aktivieren**
  Agentenrückruf ermöglicht einem Anrufer in der Warteschlange eine Sprachnachricht für Agenten zu hinterlassen. Sobald ein entsprechender Agent verfügbar wird, erhält dieser einen Anruf, hört die Sprachnachricht des Anrufers und kann ihn zurückrufen.
- **Nachbearbeitungszeit**
  Die Nachbearbeitungszeit ermöglicht einem Agenten nach Beenden eines Gesprächs zum Beispiel Verwaltungsaufgaben zu erledigen, bevor er den nächsten Anruf erhält.

Die **Liste der Agentenzuweisungen** zeigt Agenten mit dem Berechtigungs-Level Supervisor oder Administrator, welche Agenten welchen Warteschlangen zugeordnet sind. Agenten mit dem Berechtigungs-Level Agent sehen nur die Warteschlangen, denen sie selbst zugeordnet sind.

17.1.2 Voraussetzungen für myAgent

Um myAgent zu nutzen, muss der Client-PC des Teilnehmers eine geeignete Hardware- und Softwareausstattung haben.

INFO: Beachten Sie bitte unbedingt die aktuellen Hinweise in der Datei `ReadMe first`, die sich im Ablageverzeichnis der Installationsdateien befindet.

Telefone

myAgent kann in Verbindung mit folgenden Telefonen genutzt werden:

- OpenStage HFA
- OpenScape Desk Phone IP 35G/55G HFA
- OpenStage T
- OpenScape Personal Edition HFA
- OpenScape Business Cordless

Ältere Telefone (z. B. optiPoint 410/420/500) werden teilweise noch unterstützt. myAgent kann nicht verwendet werden mit SIP-Teilnehmern, Mobility Teilnehmern, virtuellen Teilnehmern, Gruppen oder MULAP-Teilnehmern.

Getestete und freigegebene Telefone entnehmen Sie bitte der Freigabemitteilung.

Betriebssystem

myAgent kann in Verbindung mit folgenden Betriebssystemen verwendet werden:

- Microsoft Windows 8
- Microsoft Windows 7
- Microsoft Windows Vista
- Microsoft Windows XP
- Microsoft Windows 2012, 2008 R2, 2008 und 2003 Server als Microsoft Terminal Server
- Microsoft Windows 2008 R2, 2008 und 2003 Server als Citrix XenApp 5.0 oder 6.0 Server

Zusätzliche Software

Zusätzliche Software für Berichte:

- Adobe Reader 9

Hardware Mindestanforderungen

- 2 GHz CPU
- RAM: 2 GB
  (Microsoft Windows XP: 1 GB)
  (Microsoft Windows 2003 Server: 1 GB)
- 100 Mbit/s LAN
- XGA (1024x768) Bildschirmauflösung, myPortal for Outlook: SVGA (800x600) Bildschirmauflösung

Microsoft Terminalserver, Citrix XenApp Server

myAgent kann unter den nachfolgend genannten Voraussetzungen in Microsoft Terminalserver- und Citrix-Server-Umgebungen eingesetzt werden.

INFO: Terminalserver- und Citrix-Server-Umgebungen inklusive Hosted Services und virtuelle Umgebungen liegen in der Verantwortung des Kunden.

INFO: Citrix-Server-Umgebungen können einige regionale Buchstaben (z.B. deutsche Umlaute) nicht korrekt decodieren.

Betriebssystem:

- Microsoft Windows 2012 Server als Microsoft Terminal Server
- Microsoft Windows 2008 R2 Server als Microsoft Terminal Server
- Microsoft Windows 2008 Server als Microsoft Terminal Server
- Microsoft Windows 2003 Server als Microsoft Terminal Server

- Microsoft Windows 2008 R2 Server (64 Bit) mit Citrix XenApp 6.0 und 6.5 Server (Desktop Mode)
- Microsoft Windows 2008 R2 Server (64 Bit) mit Citrix XenApp 5.0 Server (Desktop Mode)

Der Support von myAgent für Microsoft Windows XP und Microsoft Windows 2003 Server endet zeitgleich mit der Betreuungseinstellung durch Microsoft. Das Produkt wird weiterhin unterstützt, jedoch nicht mehr detailliert getestet.

Hardware-Voraussetzungen: Die Anzahl der installierbaren Clients hängt ab von der Server-Performance und dem zur Verfügung stehenden Arbeitsspeicher. Werden auf dem Server weitere Applikationen genutzt, ist deren Arbeitsspeicherbedarf zu berücksichtigen.

Weitere Informationen über die Konfiguration unter Citrix XenApp Server finden Sie unter:

`http://wiki.unify.com/wiki/OpenScape_Business`.

Installationsdateien

Für die Bereitstellung der Installationsdateien an die Benutzer bestehen folgende Möglichkeiten:

- Der Administrator lädt die Installationsdateien aus dem **Service-Center** herunter und stellt diese den Benutzern bereit, zum Beispiel über ein Netzlaufwerk.

Beachten Sie die Hinweise in der Datei `ReadMe first`, die sich im Ablageverzeichnis der Installationsdateien befindet.

> ***INFO:*** Die automatische Verteilung der MSI-Datei über einen Deploymentdienst mit Microsoft Windows Server wird nicht unterstützt.

17.1.3 myReports

Agenten mit dem Berechtigungs-Level Supervisor oder Administrator können mit myReports Berichte über Agenten und deren Aktivitäten, über Anrufe, Warteschlangen, Leistung, Servicelevel und Nachbearbeitungscodes erstellen.

myReports bietet folgende Leistungsmerkmale:

- Mehr als 100 vordefinierte und nach Themengebieten (Berichtgruppen) sortierte Berichtsvorlagen für die Erstellung von Berichten
- Zeitpläne für die zeitgesteuerte Erstellung von Berichten
- Sofortiger oder zeitgesteuerter Versand von Berichten per E-Mail
- Zeitgesteuerter Export von Berichten
- Ausgabeformate für die Berichtsvorschau, den E-Mail-Versand und den Export von Berichten: Excel, PDF und Word
- Berichtsvorschau für die Prüfung eines zu erstellenden Berichts im gewünschten Ausgabeformat

- Integrierter Berichts-Designer für die Definition eigener Berichtsvorlagen durch den myReports-Administrator

Benutzerrollen

myReports besitzt eine eigene Benutzerverwaltung, die den Zugriff auf die Funktionen von myReports durch Benutzerrollen regelt. Dabei wird zwischen dem myReports-Benutzer (Standardbenutzer) und dem myReports-Administrator unterschieden.

Die aktuelle Benutzerrolle wird bei der Anmeldung an myReports festgelegt.

Die Unterschiede zwischen den Benutzerrollen sind in der folgenden Tabelle zusammengefasst.

myReports: Tätigkeit	Benutzerrolle	
	myReports-Benutzer	myReports-Administrator
Berichte		
Berichtsvorschau anzeigen	X	X
Bericht sofort per E-Mail senden	X	X
Berichtsvorlage hinzufügen	X	X
Hinzugefügte Berichtsvorlage löschen	X	X
Berichts-Designer starten		X
Neue Berichtsvorlage definieren		X
Vordefinierte Berichtsvorlagen aktualisieren		X
Zeitpläne		
Zeitplan hinzufügen	X	X
Details eines Zeitplans anzeigen	X	X
Zeitplan bearbeiten	X	X
Zeitplan löschen	X	X
Konfiguration		

myReports: Tätigkeit	Benutzerrolle	
	myReports-Benutzer	myReports-Administrator
Sprache der Benutzeroberfläche ändern	X	X
Farbe der Benutzeroberfläche ändern	X	X
E-Mail-Vorlage konfigurieren	X[1]	X
Serveradresse ändern	X	X
Administrator-Kennwort ändern		X
E-Mail-Konto für Versand konfigurieren		X
Vorwahlen für externe Rufnummern konfigurieren		X
Datenschutz aktivieren/deaktivieren		X
Speicherort für den Export zeitgesteuerter Berichte konfigurieren		X
Sprache einrichten		X[2]
Standard-Sprache einrichten		X[2]

1 Für die Konfiguration der E-Mail-Vorlage ist die Eingabe des Administrator-Kennworts erforderlich.
2 Für die Einrichtung der Sprache und der Standard-Sprache ist die Anmeldung als myReports-Administrator mit einem speziellen Kennwort erforderlich.

17.1.3.1 Wie Sie myReports-Administrator-Kennwort zurücksetzen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Applikationen > OpenScape Business UC Suite**.

3) Klicken Sie auf **Server**.

4) Klicken Sie auf **Wartung**.

5) Klicken Sie auf **Kennwort zurücksetzen**.

Nächste Schritte

Informieren Sie den oder die myReports-Administratoren über das Zurücksetzen des Administrator-Kennworts auf das Standardkennwort `reports`.

17.1.4 Voraussetzungen für myReports

Um myReports zu nutzen muss der Client-PC des Teilnehmers eine geeignete Hardware- und Softwareausstattung haben.

> ***INFO:*** Beachten Sie bitte unbedingt die Hinweise in der Datei `ReadMe first`, die sich im Ablageverzeichnis der Installationsdateien befindet.

Betriebssystem

myReports kann in Verbindung mit folgenden Betriebssystemen verwendet werden:

- Microsoft Windows 8
- Microsoft Windows 7
- Microsoft Windows Vista
- Microsoft Windows XP
- Microsoft Windows 2012, 2008 R2, 2008 und 2003 Server als Microsoft Terminal Server
- Microsoft Windows 2008 R2, 2008 und 2003 Server als Citrix XenApp 5.0 oder 6.0 Server

> ***INFO:*** Das verwendete Betriebssystem benötigt stets den aktuellen Stand aller verfügbaren Updates (Service Packs und Patches).

Der Support von myReports für Microsoft Windows XP und Microsoft Windows 2003 Server endet zeitgleich mit der Betreuungseinstellung durch Microsoft. Das Produkt wird weiterhin unterstützt, jedoch nicht mehr detailliert getestet.

Zusätzliche Software

- aktuellste Java Runtime Environment Version
- Adobe Reader 9 oder höher (für Berichte im PDF-Format)
- Microsoft Excel 2013, 2010, 2007 oder 2003 (für Berichte im Excel-Format)
- Microsoft Word 2013, 2010, 2007 oder 2003 (für Berichte im Word-Format)

Hardware Mindestanforderungen

- 2 GHz CPU
- RAM: 2 GB
  (Microsoft Windows XP: 1 GB)
  (Microsoft Windows 2003 Server: 1 GB)
- 100 Mbit/s LAN (1 Gbit/s LAN empfohlen)
- XGA (1024x768) Bildschirmauflösung, myPortal for Outlook: SVGA (800x600) Bildschirmauflösung

Multiuser PC

Unter Microsoft Windows 7 mit Multiuser-PC und Microsoft Windows Vista mit Multiuser-PC kann jeder lokale Benutzer myReports mit seinen individuellen Einstellungen verwenden, wenn der erste lokale Benutzer mit lokalen Administrationsrechten dieses installiert. Nur der erste lokale Benutzer mit lokalen Administrationsrechten kann Updates per AutoUpdate durchführen.

Microsoft Terminalserver, Citrix XenApp Server

myReports kann unter den nachfolgend genannten Voraussetzungen in Microsoft Terminalserver- und Citrix-Server-Umgebungen eingesetzt werden.

INFO: Terminalserver- und Citrix-Server-Umgebungen inklusive Hosted Services und virtuelle Umgebungen liegen in der Verantwortung des Kunden.

INFO: Citrix-Server-Umgebungen können einige regionale Buchstaben (z.B. deutsche Umlaute) nicht korrekt decodieren.

Betriebssystem:

- Microsoft Windows 2012 Server als Microsoft Terminal Server
- Microsoft Windows 2008 R2 Server als Microsoft Terminal Server
- Microsoft Windows 2008 Server als Microsoft Terminal Server
- Microsoft Windows 2003 Server als Microsoft Terminal Server
- Microsoft Windows 2008 R2 Server (64 Bit) mit Citrix XenApp 6.0 und 6.5 Server (Desktop Mode)
- Microsoft Windows 2008 R2 Server (64 Bit) mit Citrix XenApp 5.0 Server (Desktop Mode)

Hardware-Voraussetzungen: Die Anzahl der installierbaren Clients hängt ab von der Server-Performance und dem zur Verfügung stehenden Arbeitsspeicher. Werden auf dem Server weitere Applikationen genutzt, ist deren Arbeitsspeicherbedarf zu berücksichtigen.

Weitere Informationen über die Konfiguration unter Citrix XenApp Server finden Sie unter:

`http://wiki.unify.com/wiki/OpenScape_Business`.

Installationsdateien

Für die Bereitstellung der Installationsdateien an die Benutzer bestehen folgende Möglichkeiten:

- Der Administrator lädt die Installationsdateien aus dem **Service-Center** herunter und stellt diese den Benutzern bereit, zum Beispiel über ein Netzlaufwerk.

Beachten Sie die Hinweise in der Datei `ReadMe first`, die sich im Ablageverzeichnis der Installationsdateien befindet.

INFO: Die automatische Verteilung der MSI-Datei über einen Deploymentdienst mit Microsoft Windows Server wird nicht unterstützt.

17.1.5 Hinweise zur gleichzeitigen Nutzung von myAgent und UC Suite Clients

Bei gleichzeitiger Nutzung von myAgent und UC Suite Clients über ein UC Suite Benutzerkonto ist eine gegenseitige Beeinflussung nicht ausgeschlossen.

Der Begriff myPortal wird in diesem Abschnitt stellvertretend für myPortal for Desktop, myPortal for Outlook, myPortal for Mobile, myPortal to go und myPortal for OpenStage verwendet.

Beispiele gegenseitiger Beeinflussung:

- Änderung des Anwesenheitsstatus über myPortal
  Die Beispiele gelten für die Standardeinstellung **Sprachnachrichten** für alle Anrufweiterleitungsziele.
  - myAgent: Agent ist angemeldet.
    myPortal: Das automatische Zurücksetzen des Anwesenheitsstatus auf Büro ist deaktiviert.
    Eine Änderung des Anwesenheitsstatus über myPortal bewirkt ein sofortiges Abmelden des Agenten von der oder den Warteschlangen. Nach dem Anmelden des Agenten über myAgent wird der Anwesenheitsstatus in myPortal wieder auf **Büro** gesetzt.
    Eine Änderung des Agentenstatus über myAgent (zum Beispiel **Pause**) wird durch myPortal registriert, mit Ausnahme von **Anmelden**, **Abmelden** und **Nachbearbeitung**.
  - myAgent: Agent ist angemeldet.
    myPortal: Das automatische Zurücksetzen des Anwesenheitsstatus auf Büro ist aktiviert.
    Ändert der Agent seinen Status über myAgent in **Pause**, ist er nach Ablauf der Pausenzeit automatisch wieder verfügbar.
    Eine Änderung des Anwesenheitsstatus über myPortal in **Pause** bewirkt ein sofortiges Abmelden des Agenten von der oder den Warteschlangen.
  - myAgent: Agent ist angemeldet.
    Eine Änderung des Anwesenheitsstatus über myPortal in **Anrufschutz** bewirkt ein sofortiges Abmelden des Agenten von der oder den Warteschlangen.
- Gehende Anrufe über myPortal
  Der Anwesenheitsstatus des Teilnehmers ist über myAgent sichtbar.
  Die Anrufe erscheinen ausschließlich im Journal von myPortal. Eine Übernahme in die Statistik des Contact Centers erfolgt nicht, da es sich nicht um Contact Center Anrufe handelt.

- Kommende Anrufe an die Teilnehmerrufnummer des Agenten
  Der Anwesenheitsstatus des Teilnehmers ist über myAgent sichtbar.
  Die Anrufe erscheinen ausschließlich im Journal von myPortal. Eine Übernahme in die Statistik des Contact Centers erfolgt nicht, da es sich nicht um Contact Center Anrufe handelt.
- Anruf aufzeichnen
  Das Aufzeichnen von Anrufen über myPortal wird nicht durch myAgent registriert. myAgent bietet diese Funktion an, auch wenn die Aufzeichnung eines Anrufs bereits über myPortal erfolgt.

17.2 Agenten

Die zu einer Warteschlange gehörenden Agenten (Teilnehmer) bilden eine Arbeitsgruppe, die zum Beispiel bei technischen Hotlines oder in der Auftrags- und Bestellannahme zum Einsatz kommen kann. Die kommenden Anrufe, Faxe und E-Mails werden gleichmäßig auf die verfügbaren Agenten einer Warteschlange verteilt.

Um einen Teilnehmer des Kommunikationssystems als Agent zu verwenden, muss dieser Teilnehmer als Agent konfiguriert werden. Die Rechte des Agenten werden dabei durch Auswahl des Berechtigungs-Levels definiert (Agent, Supervisor oder Administrator). Ein Agent mit dem Berechtigungs-Level Supervisor oder Administrator verfügt über erweiterte Berechtigungen (siehe *Administratordokumentation, Multimedia Contact Center*).

Ein Agent kann als dauerverfügbarer Agent definiert werden. Er bleibt dadurch auch dann für Anrufe, Faxe und E-Mails verfügbar, wenn er einen Anruf, ein Fax oder eine E-Mail nicht angenommen hat.

17.2.1 Berechtigungsabhängige Funktionen für Agenten

Bei der Konfiguration eines Teilnehmers als Agent werden die Rechte des Agenten durch Auswahl des Berechtigungs-Levels definiert (Agent, Supervisor oder Administrator). Ein Agent mit dem Berechtigungs-Level Supervisor oder Administrator verfügt über erweiterte Berechtigungen.

Die Unterschiede zwischen den Berechtigungs-Levels sind in der folgenden Tabelle zusammengefasst.

myAgent: Tätigkeit	**Berechtigungs-Level**		
	Agent	**Supervisor**	**Administrator**
Agent einer Warteschlange zuordnen	–	X	X
Agent zu anderer Warteschlange verschieben	–	X	X
Agent aus Warteschlange entfernen	–	X	X

myAgent: Tätigkeit	Berechtigungs-Level		
	Agent	Supervisor	Administrator
Zustand eines Agenten ändern	–	X	X
Liste der Agentenzuweisungen anzeigen	zugeordnete Warteschlangen	alle Warteschlangen	alle Warteschlangen
Agentenzuweisung bearbeiten	–	X	X
Liste der Contact-Center-Anrufe anzeigen	zugeordnete Warteschlangen	alle Warteschlangen	alle Warteschlangen
myAgent bei Alarm automatisch im Vordergrund aktivieren	–	X	X
Alarmton aktivieren	–	X	X
Wandanzeige (Wallboard) anzeigen	zugeordnete Warteschlangen	alle Warteschlangen	alle Warteschlangen
Diagramm Servicegrad anzeigen	zugeordnete Warteschlangen	alle Warteschlangen	alle Warteschlangen
Diagramm Durchschnittszeiten anzeigen	zugeordnete Warteschlangen	alle Warteschlangen	alle Warteschlangen
Anruf an die erste Position in einer Warteschlange verschieben	–	X	X
Anruf aufzeichnen	aktueller Anruf	alle Anrufe	alle Anrufe
Aufzeichnung eines Anruf als WAV-Datei speichern oder als WAV-Datei per E-Mail versenden	–	X	X
Fax als PDF- oder TIFF-Datei speichern oder per E-Mail versenden	–	X	X
E-Mail als EML-Datei speichern oder als EML-Datei per E-Mail versenden	–	X	X
Anruf mithören (länderabhängig)	–	X	X
Auf Anruf aufschalten	–	X	X
Anforderung für Unterstützung beantworten	–	X	X
Bericht erstellen	–	X	X
WBM öffnen	–	X	X

17.2.2 Bevorzugte Agenten

Jedem Anrufer (beispielsweise jedem anrufenden Kunden) können ein oder mehrere bevorzugte Agenten einer Warteschlange zugeordnet werden. In diesem Fall versucht das Kommunikationssystem, den Anrufer und die Rückrufwünsche dieses Anrufers zunächst an einen bevorzugten Agenten zu vermitteln.

Wurden mehrere bevorzugte Agenten festgelegt, kann eine Priorität (Reihenfolge) definiert werden, mit der die bevorzugten Agenten vermittelt werden.

Ist kein bevorzugter Agent verfügbar, wird der Anruf an einen beliebigen verfügbaren Agenten weitergeleitet.

17.2.3 Agent in mehreren Warteschlangen

Ein Agent kann mehreren Warteschlangen mit unterschiedlichem Fähigkeits-Level zugeordnet werden. Dabei ist zu definieren, ob der Agent als Hauptagent oder als Agent bei Überlauf fungieren soll.

17.2.4 Contact Center-Pausen

Um jedem Agenten definierte Pausen zu ermöglichen, können unterschiedlich lange Contact Center-Pausen festgelegt werden (zum Beispiel Mittagspause, Zigarettenpause). Contact Center-Pausen stehen systemweit zur Verfügung und können bei Bedarf von einem Agenten über myAgent ausgewählt werden.

17.3 Warteschlangen und Zeitpläne

Warteschlangen sind die Basis des Contact Centers. Anrufe, Faxe und E-Mails für eine Warteschlange können in Abhängigkeit vom Fähigkeits-Level der Agenten, von der Priorität und der Wartezeit behandelt werden. Anrufern, die sich im Wartezustand befinden, können Ansagen eingespielt werden. Über einen Zeitplan wird definiert, wie kommende Anrufe an bestimmten Tagen und zu bestimmten Zeiten behandelt werden sollen.

17.3.1 Warteschlangen

Im Regelfall erfolgt die Anrufverteilung so, dass ein kommender Anruf, ein Fax oder eine E-Mail an eine Warteschlange an denjenigen Teilnehmer in der Gruppe (Agent) weitergeleitet wird, dessen letztes Gespräch am längsten zurückliegt. Es ist ebenfalls möglich andere Verteilungsregeln festzulegen (zum Beispiel anhand der verschiedenen Fähigkeits-Level der Agenten). Sind alle Agenten belegt, werden zusätzliche Anrufe, Faxe und E-Mails in Wartestellung gebracht und anschließend in Abhängigkeit von Priorität und Wartezeit an die frei werdenden Agenten verteilt.

Anhand von Zeitplänen und den darin enthaltenen Regeln (= CCV, Call Control Vector) kann definiert werden, wie ein Anruf an eine Warteschlange zu einer

bestimmten Zeit oder an einem bestimmten Tag behandelt werden soll. Die Regeln definieren beispielsweise, welche Ansage Anrufern eingespielt wird oder wohin ein Anruf weitergeleitet wird.

Faxe, E-Mails und Agentenrückrufe werden unabhängig von Zeitplänen den Warteschlangen direkt zugeordnet.

Bei der Zuordnung von Agenten zu Warteschlangen können den Agenten verschiedene Eigenschaften zugewiesen werden (Agentenzuweisung), die Einfluss auf die Verteilung der Anrufe in einer Warteschlange haben (zum Beispiel Hauptagent oder Agent bei Überlauf, Fähigkeits-Level). Die Zuordnung von Agenten zu Warteschlangen ist möglich

- über das WBM durch einen Administrator mit dem Profil **Advanced**.
- über die Applikation myAgent durch einen Agenten mit dem Berechtigungs-Level Supervisor oder Administrator.

Ist ein Agent mehreren Warteschlangen zugeordnet, kann über die Warteschlangen-Priorität festgelegt werden, ob die Anrufe für eine Warteschlange mit höherer Priorität an diesen Agenten weitergeleitet werden sollen als die Anrufe für andere Warteschlangen.

Für Warteschlangen können folgende wesentlichen Einstellungen über das WBM vorgenommen werden:

- Warteschlangen aktivieren, deaktivieren, löschen
  Hinweis: Nach dem Löschen einer Warteschlangen können keine Berichte über vergangene Zeiträume erstellt werden. Nicht mehr benötigte Warteschlangen sollten deaktiviert werden.
- Warteschlangen-Alarme konfigurieren
  Es bestehen folgende Möglichkeiten:
  - Anzahl Warteschlangen-Alarme (Alarm-Schwellwertanzahl): Wird die hier angegebene Anzahl wartender Anrufe in der Warteschlange überschritten, wechselt das Warteschlangensymbol bei den Agenten von grün auf orange. Agenten mit dem Berechtigungs-Level Supervisor oder Administrator können einstellen, ob sie durch einen Alarmton gewarnt werden sollen und ob myAgent automatisch im Vordergrund erscheinen soll.
  - Zeit Warteschlangen-Alarm (Alarm-Schwellwertzeit): Wird die hier angegebene Wartezeit eines Anrufs in der Warteschlange überschritten, wechselt der betreffende Eintrag in der Liste der Contact-Center-Anrufe bei den Agenten auf rot. Agenten mit dem Berechtigungs-Level Supervisor oder Administrator können einstellen, ob sie durch einen Alarmton gewarnt werden sollen und ob myAgent automatisch im Vordergrund erscheinen soll.
- Zeitüberschreitung für entgangene Anrufe, Faxe und E-Mails definieren
  Wird ein Anruf, ein Fax oder eine E-Mail nach Ablauf der hier angegebenen Zeit vom Agenten nicht angenommen, wird der Anruf, das Fax oder die E-Mail zum nächsten freien Agenten weitergeleitet.
- Schwellwert für abgebrochene Anrufe definieren
  Anhand der angegebenen Zeit wird festgelegt, ob ein abgebrochener Anruf in die Statistik (in einen Bericht) aufgenommen wird oder nicht. Statistisch

erfasst werden Anrufe, die nach Ablauf der angegebenen Zeit abgebrochen werden.

- Pilots für eingehende Faxnachrichten einrichten
  Falls eingerichtet, können Rufnummern für eingehende Faxnachrichten ausgewählt werden. Faxe an diese Rufnummern werden in die Warteschlange übernommen und wie kommende Anrufe behandelt.
- Dienst für eingehende E-Mails einrichten
  Für eine Warteschlange können mehrere E-Mail-Adressen eingerichtet werden. E-Mails an diese Adressen werden in die Warteschlange übernommen und wie kommende Anrufe behandelt.
- Absender-E-Mail-Adresse einrichten
  E-Mail-Adresse der Warteschlange, die beim Versenden einer E-Mail durch einen Agenten beim Empfänger angezeigt wird.
- Intelligente Anrufweiterleitung aktivieren
  Ein kommender Anruf wird an den Agenten weitergeleitet, der zuletzt mit dem Anrufer verbunden war. Vorausgesetzt, für diesen Anrufer wurden keine bevorzugten Agenten definiert.

17.3.2 Zeitpläne

Für jede Warteschlange wird über einen Zeitplan und die darin enthaltenen Regeln (Call Control Vector CCV) definiert, wie kommende Anrufe an bestimmten Tagen und zu bestimmten Zeiten behandelt werden sollen.

Beispielsweise kann für Werktage eine Regel für die Frühschicht (von 6:00 Uhr bis 14:00 Uhr), eine für die Mittagschicht (14:00 Uhr bis 22:00 Uhr) und eine für die Nachtschicht (von 22:00 bis 06:00 Uhr) definiert werden. Für das Wochenende kann eine Wochenendregel definiert werden. Für jede dieser Regeln kann zum Beispiel angegeben werden, ob eine Ansage abgespielt und/oder wohin Anrufe weitergeleitet werden sollen.

Zeitpläne sind das Kernstück der Contact-Center-Einrichtung. Ohne die Definition mindestens eines Zeitplans kann die Einrichtung eines Contact Centers nicht erfolgreich beendet werden. Jeder Warteschlange muss mindestens ein Zeitplan zugewiesen worden sein. Das kann auch immer derselbe Zeitplan sein.

Einem Zeitplan muss mindestens eine Regel (Call Control Vector CCV) zugeordnet werden. Die Regeln bestimmen für den Zeitraum für den ein Zeitplan gilt, wie kommende Anrufe in einer Warteschlange behandelt werden. Regeln gelten ausschließlich für Anrufe und nicht für Faxe und E-Mails.

Regeln werden mit dem graphischen Regel-Editor (CCV-Editor) durch die Verknüpfung von vordefinierten CCV-Objekten erstellt und können nach der Fertigstellung unter einem frei definierbaren Namen gespeichert werden.

Gespeicherte Regeln können einem oder auch mehreren Zeitplänen als Standard-Regel (Standard-CCV) oder Ausnahme-Regel (Ausnahme-CCV) zugeordnet werden. Das Öffnen, Modifizieren und erneute Speichern über den Regel-Editor ist jederzeit möglich.

Wurde einem Zeitplan eine Standard-Regel (Standard-CCV) zugeordnet, kann dieser Zeitplan unter einem frei definierbaren Namen gespeichert werden. Ein Zeitplan mit einer Standard-Regel gilt nach Zuweisung zu einer Warteschlange 24 Stunden am Tag und 365 Tage im Jahr. Sollen zu bestimmten Zeiten (Pause, Wochenende, Feiertag, Urlaub usw.) andere Regeln gelten, können diese dem entsprechenden Zeitplan als Ausnahme-Regeln (Ausnahme-CCV) zugeordnet werden. Damit kann für jede Warteschlange definiert werden, wie kommende Anrufe beispielsweise während der Urlaubszeit behandelt werden sollen. Urlaubspläne haben hierbei Vorrang vor anderen Zeitplänen und Regeln einer Warteschlange.

Regel-Editor (CCV-Editor)

Mit dem Regel-Editor können aus vordefinierten CCV-Objekten Regeln gebildet werden. Die Anordnung der CCV-Objekte und deren Eigenschaften bestimmen, wie kommende Anrufe behandelt werden.

Folgende vordefinierte CCV-Objekte stehen zur Verfügung:

INFO: Für alle genannten CCV-Objekte gelten zusätzlich die beiden folgenden allgemeinen Eigenschaften:

Beschreibung: Optionale Möglichkeit das CCV-Objekt zu beschreiben, wie zum Beispiel Begrüßungsansage.

Aktion nach Zifferneingabe: Angabe der benötigten Ziffer(n) ohne Leerzeichen, Kommas oder anderer Zeichen. Die Angabe bezieht sich auf das vorherige CCV-Objekt. Wurde dort unter Mögliche Ziffern 9 angegeben, muss auch hier 9 stehen.

- **Nachricht abspielen**
  Bewirkt das Abspielen der gewünschten Ansage. Ausgewählt werden kann eine in der UC Suite vorliegende Audiodatei. Darüber hinaus kann eine neue Audiodatei in die UC Suite importiert werden oder eine neue Ansage aufgezeichnet und anschließend als Audiodatei in die UC Suite importiert werden.
  Durch das Abspielen der Ansage wird jeweils ein Media Stream Channel belegt.
  Eigenschaften:
  – **Dateiname**: Auswahl einer Ansage (Audiodatei im wav-Format)
  – **Abbruchtasten**: Angabe einer Taste oder Tastenkombination auf der Wähltastatur, mit der ein Anrufer das Abspielen der Ansage abbrechen kann.
  – **Datei-Manager**: Über diese Schaltfläche ist es direkt möglich, eine Audio-Datei im wav-Format hochzuladen bzw. mit dem Aufzeichnungsgerät eine neue Sprachdatei zu erzeugen.
- **Wartemusik**
  Bewirkt das Einspielen von Wartemusik (Music On Hold MOH des Kommunikationssystems) für externe Anrufer für eine einstellbare Zeit
  Eigenschaft:
  – **Zeitwert**: Zeit in Sekunden, über die die Wartemusik eingespielt werden soll.

- **Verbindung mit Anrufer trennen**
  Bewirkt das Beenden der Verbindung
  Nach diesem CCV-Objekt kann kein weiteres CCV-Objekt mehr eingefügt werden.
- **Anrufer über Warteschlangenposition informieren**
  Bewirkt die Information des Anrufers über seine aktuelle Warteschlangenposition
- **Zu CCV**
  Bewirkt eine Schleife zu einem anderen CCV-Objekt
  Eigenschaft:
  – **Ziel-CCV**: Auswahl des CCV-Objekts
- **Callback aufzeichnen**
  Ermöglicht einem Anrufer in einer Warteschlange einen Agentenrückruf zu aktivieren (Aufnahme einer Sprachnachricht). Der Agentenrückruf bleibt anstelle des eigentlichen Anrufers in der Warteschlange. Agenten mit der Merkmal **Agentenrückruf aktivieren** wird der Agentenrückruf in der Liste der Contact-Center-Anrufe angezeigt.
  Nach diesem CCV-Objekt kann kein weiteres CCV-Objekt mehr eingefügt werden.
  Eigenschaften:
  – **Typ**: Auswahl von **Einfacher Rückruf** oder **Extensiver Rückruf**.
    Im Gegensatz zu einem einfachen Rückruf stehen einem Anrufer bei einem extensiven Rückruf zusätzliche Möglichkeiten und Informationen zur Verfügung (Bestätigung oder Änderung der Rufnummer an die der Rückruf erfolgen soll, Bestätigung der Sprachnachricht).
  – **Max. Nachrichtenlänge**: Zeit in Sekunden, die einem Anrufer für die Aufnahme einer Sprachnachricht zur Verfügung steht.
- **Aktion nach Zifferneingabe ausführen**
  Bewirkt die Ausführung des oder der nachfolgenden CCV-Objekte in Abhängigkeit von den dort angegebenen Ziffern (Aktion nach Zifferneingabe).
  Eigenschaften:
  – **Dateiname**: Auswahl einer oder mehrerer Ansagen (Audiodatei im wav-Format)
  – **Wiedergabeliste**: Liste der ausgewählten Ansagen (Audiodatei im wav-Format) in der Reihenfolge der Wiedergabe
  – **Zeitüberschreitung bei Zifferneingabe**: Zeit in Sekunden, innerhalb der das Kommunikationssystem auf die Zifferneingabe wartet.
    Erfolgt die vollständige Zifferneingabe nicht innerhalb der angegebenen Zeit, wird die Nachricht (Ansage) erneut abgespielt.
  – **Link an**: Auflistung der Ziffer mit Ziel.
    Die Ziffern und Ziele können hinzugefügt, bearbeitet und entfernt werden.
  – **Datei-Manager**: Über diese Schaltfläche ist es direkt möglich, eine Audio-Datei im wav-Format hochzuladen bzw. mit dem Aufzeichnungsgerät eine neue Sprachdatei zu erzeugen.
  Der Inhalt der Wiedergabeliste wird im Regel-Editor anhand eines Tooltips angezeigt, wenn man mit dem Mauszeiger auf dem CCV-Objekt verweilt.

- **Einzelschritt-Übergabe**
  Die Funktion ist abhängig von der Einstellung **Normales Vermittlungsplatz-SST** (WBM, **Experten-Modus**: **Applikationen > OpenScape Business UC Suite > Server > Allgemeine Einstellungen**):
  – **Normales Vermittlungsplatz-SST** aktiviert (Standardeinstellung, nicht für USA): Bewirkt die Übergabe des Anrufs, unabhängig davon, ob das Ziel frei, besetzt oder nicht verfügbar ist.

    INFO: Bei einem Teilnehmer mit Anklopfschutz wird der Anruf erst vermittelt, wenn der Zielteilnehmer frei ist. Ein Anklopfen im Besetztfall erfolgt nicht.

  – **Normales Vermittlungsplatz-SST** deaktiviert (Standardeinstellung, nur für USA): Bewirkt eine Übergabe des Anrufs, wenn das Ziel frei ist.
    Ist das Ziel besetzt und der Anklopfschutz deaktiviert oder ist das Ziel nicht verfügbar, wird dem Anrufer eine Ansage eingespielt. Dabei kann der Anrufer wählen, ob er eine Nachricht auf der Sprachbox des Teilnehmers hinterlassen möchte oder ob er die Rufnummer eines anderen Ziels wählen möchte.
    Ist das Ziel besetzt und der Anklopfschutz aktiviert, erfolgt keine Vermittlung des Anrufs.

  Nach diesem CCV-Objekt kann kein weiteres CCV-Objekt mehr eingefügt werden.
  Eigenschaft:
  – **Zielnebenstelle**: Angabe der internen Rufnummer oder der externen Durchwahl mit Amtsleitungsnummer. Leerzeichen, Kommas oder andere Zeichen sind nicht erlaubt.

  Die Rufnummer der Zielnebenstelle wird im CCV-Objekt angezeigt.
- **An Warteschlange übergeben**
  Bewirkt die Übergabe des Anrufs an eine Warteschlange
  Nach diesem CCV-Objekt kann kein weiteres CCV-Objekt mehr eingefügt werden.
  Eigenschaft:
  – **Warteschlange**: Auswahl der Warteschlange
- **In Mailbox aufzeichnen**
  Bewirkt den Anruf an die gewünschte Sprachbox eines Teilnehmers oder einer Sprachbox-Gruppe
  Nach diesem CCV-Objekt kann kein weiteres CCV-Objekt mehr eingefügt werden.
  Eigenschaft:
  – **Benutzer-Mailbox**: Angabe der Rufnummer der Sprachbox eines Teilnehmers oder einer Sprachbox-Gruppe

  Die Rufnummer und der Name der Sprachbox oder der Sprachbox-Gruppe werden im Regel-Editor anhand eines Tooltips angezeigt, wenn man mit dem Mauszeiger auf dem CCV-Objekt verweilt.

- **Übergabe nach Melden**
  Bewirkt die Übergabe des Anrufs an ein internes Ziel. Während der Übergabe wird dem Anrufer Wartemusik (Music On Hold MOH der UC Suite) eingespielt.
  Im Gegensatz zum CCV-Objekt Einzelschritt-Übergabe müssen hier zwei weitere CCV-Objekte eingefügt werden. Es muss nämlich definiert werden, wie sich das Kommunikationssystem verhalten soll, wenn das Anrufziel besetzt ist oder der Anruf nicht angenommen wird. Üblicherweise wird dem Anrufer in diesen Fällen eine Ansage eingespielt.
  Eigenschaften:
  - **Zielnebenstelle**: Angabe der internen Rufnummer.
    Es werden nur interne Rufnummern im eigenen Knoten unterstützt. Das Weiterleiten auf externe Ziele, virtuelle Teilnehmer, weitere AutoAttendants, UCD inkl. Contact Center, Mobility Teilnehmer sowie externe CallMe-Ziele ist nicht zulässig! Für diese Szenarien ist der SST (Einzelschritt Übergabe) zu verwenden.
  - **Zeitüberschreitung beim Klingeln**: Zeit in Sekunden, innerhalb der der Anruf angenommen werden muss.
    Wird der Anruf nicht innerhalb der angegebenen Zeit angenommen, wird dieser zum Kommunikationssystem zurückgestellt und das nächste CCV-Objekt verwendet.

    INFO: Die hier angegebene Zeit muss kürzer sein als die für die Rufweiterschaltung konfigurierte Zeit (Standardeinstellung für die Rufweiterschaltung = 15 Sekunden). Siehe *Administratordokumentation, Funktionen am Telefon*.

  - **Anruf zurücknehmen, wenn Zielgerät weitergeleitet/umgeleitet ist**: Option (gilt nur für interne Rufnummer)
    Bei aktivierter Option erfolgt eine Prüfung des Anrufziels. Wurde für das Anrufziel eine Anrufweiterschaltung oder Anrufumleitung aktiviert, wird der Anruf zum Kommunikationssystem zurückgestellt und das nächste CCV-Objekt verwendet.
  - **Anwesenheitsstatus bei der Anrufübergabe prüfen**: Option
    Bei aktivierter Option erfolgt eine Prüfung des Anwesenheitsstatus des Anrufziels. Bei einem anderen Anwesenheitsstatus als Büro wird auf die Sprachbox des Anrufziels umgeleitet.
- **Nach Name wählen**
  Bewirkt die Aufforderung des Anrufers, die ersten drei Buchstaben des gewünschten Teilnehmer-Nachnamens über die Wähltastatur einzugeben. Gibt es einen Teilnehmer mit den eingegebenen Anfangsbuchstaben, wird eine Verbindung hergestellt.
  Gibt es mehrere Teilnehmer mit den eingegebenen Anfangsbuchstaben, werden dem Anrufer die Namen dieser Teilnehmer angesagt (maximal 10 Teilnehmer). Hat ein Teilnehmer keine Namensansage aufgezeichnet, wird stattdessen die Rufnummer angesagt. Nach der Auswahl des gewünschten Teilnehmers wird eine Verbindung hergestellt.
  Entspricht kein Teilnehmer den eingegebenen Anfangsbuchstaben, erhält der Anrufer eine entsprechende Meldung.

INFO: Die Tasten der Wähltastatur reagieren auf den ersten Tastendruck. Mit jedem Tastendruck wird geprüft, ob es Teilnehmer-Nachnamen mit den der Taste zugeordneten Buchstaben gibt.

Beispiel: Im internen Verzeichnis gibt es die folgenden fünf Nachnamen mit den Anfangsbuchstaben t, u und v: Taylor, Taler, Ullrich, Vasquez und Volterra. Um ein Verbindung mit dem Teilnehmer Taylor herzustellen, sind folgende Tasten zu betätigen: 8 2 9

Nach diesem CCV-Objekt kann kein weiteres CCV-Objekt mehr eingefügt werden.

Eigenschaften:

– **Methode**: Auswahl von **An Nebenstelle übergeben** oder **In Mailbox aufzeichnen**.

  Je nach ausgewählter Methode wird eine Verbindung zum gewünschten Teilnehmer oder zu dessen Sprachbox hergestellt. Dabei werden ausschließlich interne Teilnehmer unterstützt, die mit Vor- und Nachnamen im internen Verzeichnis eingetragen sind.

- **Nebenstellenwahl**

  Bewirkt die Aufforderung des Anrufers, die Rufnummer des gewünschten Teilnehmers über die Wähltastatur einzugeben.

  Wählt der Anrufer die Rufnummer eines virtuellen Teilnehmers, wird er aufgefordert eine andere Teilnehmer-Rufnummer einzugeben. Anschließend wird eine Verbindung hergestellt. Meldet sich der gewünschte Teilnehmer nicht, nimmt dessen Sprachbox den Anruf entgegen.

  Nach diesem CCV-Objekt kann kein weiteres CCV-Objekt mehr eingefügt werden.

  Eigenschaften:

  – **Methode**: Auswahl von **An Nebenstelle übergeben** oder **In Mailbox aufzeichnen**.

    Je nach ausgewählter Methode wird eine Verbindung zum gewünschten Teilnehmer oder zu dessen Sprachbox hergestellt. Dabei werden ausschließlich interne Teilnehmer unterstützt, deren Rufnummer im internen Verzeichnis eingetragen ist.

- **Sprache einstellen**

  Bewirkt die Auswahl der Sprache für die jeweilige Standardansage anhand der Rufnummer des Anrufers. Zu beachten ist, dass ausschließlich Standardansagen (Systemansagen) und keine persönlichen Ansagen berücksichtigt werden.

  Definiert werden kann zum Beispiel, dass für eine Rufnummer mit der Ländervorwahl 0049 eine deutsche Ansage und für eine Rufnummer mit der Ländervorwahl 0033 eine französische Ansage abgespielt wird.

  Eigenschaften:

  – **Standard-Sprache**: Aufklappliste zur Auswahl einer Sprache.

    Die hier ausgewählte Sprache wird für alle Rufnummern verwendet, für die selbst keine Sprache definiert wurde.

- **Muster**: Angabe der Rufnummer, der eine bestimmte Sprache zugeordnet werden soll.
  Folgende Platzhalter können verwendet werden: * = beliebige Zahl, ? = beliebige Ziffer.
- **Sprache**: Aufklappliste zur Auswahl der Sprache, die der zugehörigen Rufnummer (**Muster**) zugeordnet werden soll.

Beliebig vielen verschiedenen Rufnummern (**Muster**) kann eine Sprache zugeordnet werden.

- **CLI Routing**
  Bewirkt die Weiterleitung eines Anrufs an ein oder mehrere, aufeinander folgende CCV-Objekte anhand der Rufnummer des Anrufers.
  Definiert werden kann zum Beispiel, dass für eine Rufnummer mit der Ländervorwahl 0049 zuerst eine deutsche Ansage abgespielt werden soll (CCV-Objekt **Nachricht abspielen**) und der Anruf anschließend an eine internes Telefon weitergeleitet werden soll (CCV-Objekt **Einzelschritt-Übergabe**).
  Eigenschaften:
  - **Standard**: Aufklappliste zur Auswahl des CCV-Objekts.
    Das hier ausgewählte CCV-Objekt wird für alle Rufnummern verwendet, für die selbst kein Ziel definiert wurde.
  - **Muster**: Angabe der Rufnummer, der ein bestimmtes CCV-Objekt als Ziel zugeordnet werden soll.
    Folgende Platzhalter können verwendet werden: * = beliebige Zahl, ? = beliebige Ziffer.
  - **Beschreibung**:
    Angabe einer Erläuterung.
    Für das **Muster** 0049 (= Ländervorwahl Deutschland) kann zum Beispiel Deutschland eingegeben werden.
    Der hier eingegebene Text wird im Regel-Editor angezeigt.
  - **Ziel**: Aufklappliste zur Auswahl des CCV-Objekts, das der zugehörigen Rufnummer (**Muster**) als Ziel zugeordnet werden soll.

  Beliebig vielen verschiedenen Rufnummern (**Muster**) kann ein CCV-Objekt als Ziel zugeordnet werden.
- **Bedingte Verzweigung**
  Bewirkt die Weiterleitung eines Anrufs an ein oder mehrere, aufeinander folgende CCV-Objekte anhand einer Bedingung.
  Definiert werden kann zum Beispiel, dass Anrufern eine Ansage eingespielt wird (Bitte rufen Sie zu einem späteren Zeitpunkt noch einmal an ...), sobald sich mehr als 20 Anrufe in einer Warteschlange befinden.
  Eigenschaften:
  - **Variable**: Auswahl von **Anrufe** oder **Verfügbare Agenten**.
    Je nach ausgewählter Variablen wird als Bedingungsvorgabe die Anzahl der wartenden Anrufe in einer Warteschlange oder die Anzahl der verfügbaren Agenten (inklusive Agenten in der Nachbearbeitungszeit) einer Warteschlange verwendet. In der zugehörigen Aufklappliste ist die Bedingung (**kleiner als**, **größer als**, **kleiner oder gleich als**, **größer oder gleich als**, **gleich als**) auszuwählen und in dem zugehörigen Eingabefeld ist der Vergleichswert einzugeben.

- **Bedingung erfüllt**: Aufklappliste zur Auswahl des CCV-Objekts, das bei erfüllter Bedingung als Ziel verwendet werden soll.
- **Bedingung nicht erfüllt**: Aufklappliste zur Auswahl des CCV-Objekts, das bei nicht erfüllter Bedingung als Ziel verwendet werden soll.

Die Anzahl der verfügbaren Agenten in einer Warteschlange wird durch folgende Statusänderungen der Agenten beeinflusst:

- Anmelden eines Agenten in die Warteschlange über "Anmelden/Login": --> +1
- Abmelden eines Agenten aus der Warteschlange über "Abmeldung/ Logout": --> -1
- Agent im Zustand "Pause": --> -1
- Agent im Zustand "Verfügbar nach Pause": --> +1

Die Anzahl der verfügbaren Agenten in einer Warteschlange wird durch folgende Statusänderungen der Agenten **nicht** beeinflusst:

- Agent im Zustand "Klingeln"
- Agent im Zustand "Gespräch"
- Agent in Zustand "Nachbearbeitung"
- Agent im Zustand "Verpasster Anruf"
- Agent im Zustand "Überfällig"

17.3.3 Nachbearbeitung

Anhand von Nachbearbeitungsgründen können kommende Anrufe bestimmten Themen (Bestellung, Reklamation, Service usw.) zugeordnet werden. Die Zuordnung trifft ein Agent nach Gesprächsende (in der Nachbearbeitungszeit) über myAgent, durch Auswahl des betreffenden Nachbearbeitungsgrunds.

Nachbearbeitungsgründe können für jede Warteschlange individuell definiert werden.

Unterschieden wird zwischen

- einfacher Nachbearbeitung
  Für Warteschlangen mit dem Nachbearbeitungsmodus "Einfache Nachbearbeitung" können ein oder mehrere Nachbearbeitungsgründe definiert werden.
  Beispiel: Für eine Warteschlange wurden die beiden Nachbearbeitungsgründe Hardware-Problem und Software-Problem definiert. Jeder Anruf wird in der Nachbearbeitungszeit durch einen Agenten einem dieser Nachbearbeitungsgründe zugeordnet. So kann beispielsweise ein Bericht erstellt werden, der eine Übersicht aller Anrufe zum Thema Hardware-Problem enthält.
- mehrfacher Nachbearbeitung
  Für Warteschlangen mit dem Nachbearbeitungsmodus "Mehrfache Nachbearbeitung" können ein oder mehrere Nachbearbeitungsgründe definiert und in Gruppen und Untergruppen zusammengefasst werden.
  Beispiel: Für eine Warteschlange wurde eine Gruppe Hardware mit den Nachbearbeitungsgründen Motherboard und Power Supply und eine Gruppe Software mit den Nachbearbeitungsgründen Operating System und Driver

definiert. Jeder Anruf wird in der Nachbearbeitungszeit durch einen Agenten einem dieser Nachbearbeitungsgründe zugeordnet. So kann beispielsweise ein Bericht mit einer Übersicht über alle Anrufe zu Hardware-Problemen oder auch über alle Anrufe zu Motherboard-Hardware-Problemen erstellt werden.

17.3.4 Servicegrad

Anhand des Servicegrads können Aussagen über die Beantwortungsqualität einer Warteschlange getroffen werden. Ermöglicht wird dies durch den Vergleich der Anruferwartezeiten in einer Warteschlange mit Sollwerten, die individuell für jede Warteschlange vorgegeben werden können.

Die Sollwerte für den Servicegrad (Grade Of Service GOS) können in Abhängigkeit von der Anruferwartezeit in einer Warteschlange frei bestimmt werden. Für jeden Anruf an eine entsprechende Warteschlange wird der Servicegrad nach Beendigung des Anrufs ermittelt und in die Datenbank übernommen. Eine Auswertung des Servicegrads können Agenten mit dem Berechtigungs-Level Supervisor oder Administrator über die Applikation myAgent vornehmen.

17.3.5 Wandanzeige (Wallboard)

Über myAgent kann die Anzeige der Warteschlangendetails aufgerufen werden. Diese enthält eine Tabelle mit statistischen Informationen zu Warteschlangen in Echtzeit für den aktuellen 24-Stunden-Zeitraum. Die Anzeige kann zum Beispiel über einen großen LCD-Monitor oder über einen Beamer erfolgen (Wallboard).

Ein Agent mit dem Berechtigungs-Level Agent erhält Informationen über die Warteschlangen, denen er zugeordnet ist. Ein Agent mit dem Berechtigungs-Level Supervisor oder Administrator erhält Informationen über alle Warteschlangen.

Für die Wandanzeige sollte ein separater Teilnehmer eingerichtet werden. Dafür ist eine Teilnehmer-Lizenz (IP User oder TDM User) und eine myAgent-Lizenz erforderlich.

17.3.6 Agentenrückruf

Ist einem Anrufer die Wartezeit in der Warteschlange zu lang und enthält der zugehörige Zeitplan das CCV-Objekt **Callback aufzeichnen**, kann er einen Rückrufwunsch hinterlassen. Dieser Rückrufwunsch behält die Position des ursprünglichen Anrufers in der Warteschlange und wird den Agenten in Form einer Sprachnachricht zugestellt. Nach Abhören der Sprachnachricht kann der Agent den Anrufer über ein PopUp-Fenster zurückrufen.

Wurde für einen Anrufer ein bevorzugter Agent festgelegt, wird zunächst versucht die Rückrufwünsche dieses Anrufers an den bevorzugten Agenten zu vermitteln. Ist der bevorzugte Agent nicht verfügbar, wird der Rückrufwunsch an einen beliebigen verfügbaren Agenten weitergeleitet.

17.4 VIP-Betreuung

Für jede Warteschlange kann individuell definiert werden, ob bestimmte Anrufer oder Anrufer, die einstellbaren Rufnummernmustern entsprechen, bevorzugt behandelt werden sollen und dadurch schneller einen freien Agenten erreichen sollen.

Sind alle Agenten einer Warteschlange belegt, werden VIP-Anrufer bevorzugt mit dem nächsten freien Agenten verbunden.

17.4.1 VIP-Anruferpriorität

Anhand der VIP-Anruferpriorität kann für jede Warteschlange individuell definiert werden, ob die in der VIP-Rufliste enthaltenen Anrufer (beispielsweise Kunden) bevorzugt behandelt werden sollen.

Die Werte für die VIP-Anruferpriorität können in Abhängigkeit von der Anruferwartezeit in einer Warteschlange frei bestimmt werden. Damit wird der Grad der Bevorzugung von VIP-Anrufern gegenüber normalen Anrufern festgelegt.

Aktiviert ein VIP-Anrufer einen Agentenrückruf (Aufnahme einer Sprachnachricht mit Rückrufwunsch) verbleibt der Agentenrückruf anstelle des VIP-Anrufers in der Warteschlange. Die VIP-Anruferpriorität wird dabei nicht übernommen.

VIP-Anrufer müssen in der VIP-Rufliste verzeichnet sein (siehe *VIP-Rufliste*).

17.4.2 VIP-Rufliste

Bereits im Kommunikationssystem erfasste Anrufer (externes Verzeichnis) können in die VIP-Rufliste übernommen werden. Darüber hinaus ist die Eingabe von Rufnummernmustern möglich. Rufnummernmuster setzen sich aus einer bestimmten Ziffernfolge und einer Wildcard (Platzhalter) zusammen. Damit können beispielsweise alle Mitarbeiter eines Unternehmens in die VIP-Rufliste übernommen werden.

Für jede Warteschlange kann über die VIP-Anruferpriorität definiert werden, ob

- die in der VIP-Rufliste enthaltenen Anrufer und
- die zu einem in der VIP-Rufliste enthaltenen Rufnummernmuster passenden Anrufer bevorzugt behandelt werden sollen.

Die Eingabe von Rufnummernmustern im kanonischen Rufnummernformat ist nicht möglich. Auch die Verwendung von Abkürzungszeichen für Ländervorwahlen (zum Beispiel +49 statt 0049) ist nicht möglich. Rufnummernmuster sind immer ohne Amtskennziffer anzugeben.

Beispiele für Rufnummernmuster:

- 089 7577* (089 = Ortskennzahl München, 7577 = Anlagenrufnummer eines Unternehmens, * = Wildcard für eine beliebige Zahl). Durch den Eintrag

dieses Rufnummernmusters in die VIP-Rufliste können alle Anrufer aus München, deren Rufnummer mit 7577 beginnt, bevorzugt behandelt werden.

- 0039* (0039 = Ländervorwahl Italien, * = Wildcard für eine beliebige Zahl). Durch den Eintrag dieses Rufnummernmusters in die VIP-Rufliste können alle Anrufer aus Italien bevorzugt behandelt werden.

Folgende Zeichen können als Wildcards (Platzhalter) in einem Rufnummernmuster verwendet werden:

- * = Wildcard für eine beliebige Zahl
- ? = Wildcard für eine beliebige Ziffer

17.5 Rückfalllösung (Fallback-Lösung)

Steht das Contact Center aufgrund von Problemen (Absturz, fehlende Verbindung oder ähnliches) nicht zur Verfügung, wird automatisch auf das Leistungsmerkmal "Uniform Call Distribution UCD" des Kommunikationssystems umgeschaltet. Das Leistungsmerkmal dient damit als Rückfalllösung für das Contact Center.

Bei einem Ausfall des Contact Centers werden die kommenden Anrufe entsprechend der Rückfalllösung verteilt. Das Verteilung von Faxen und E-Mails ist nicht möglich.

Je nach Anforderung kann eine der nachfolgend beschriebenen Rückfalllösungen konfiguriert werden.

Standard-Rückfalllösung

In diesem Fall basiert die Rückfalllösung auf den UCD-IDs (Agenten-IDs) der Agenten:

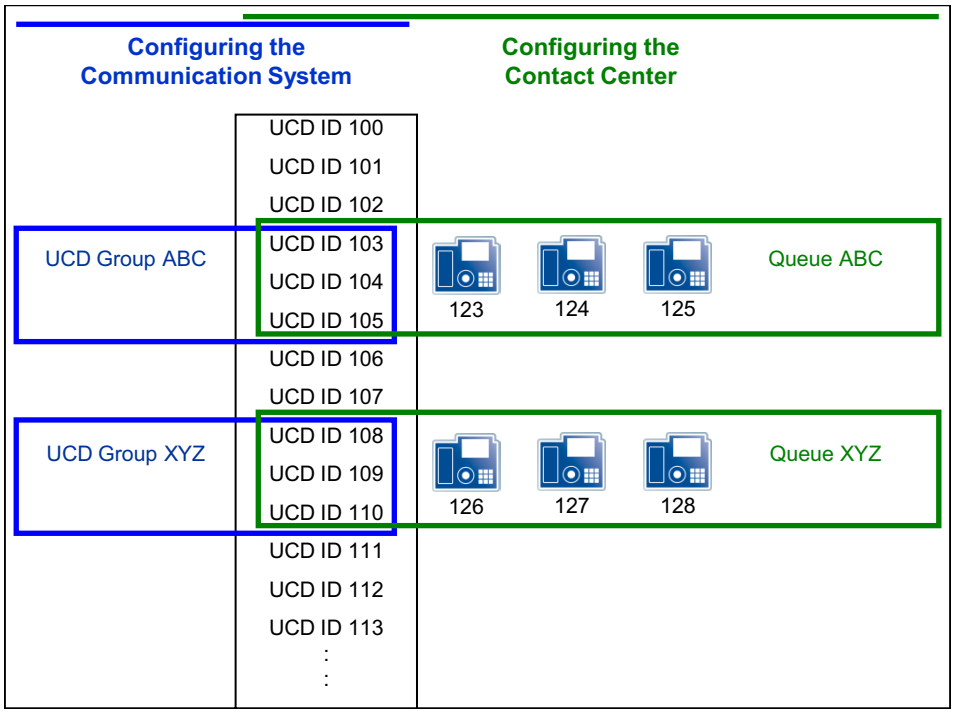
- Den UCD-Gruppen des Kommunikationssystems werden Agenten anhand von UCD-IDs zugeordnet. Die UCD-ID bestimmt, welcher UCD-Gruppe dieser Agent bei einem Ausfall des Contact Centers zugeordnet wird.

Für eine korrekte Funktion der Standard-Rückfalllösung müssen jeder Warteschlange die Contact-Center-Agenten mit den UCD-IDs zugeordnet werden, die den entsprechenden UCD-Gruppen zugeordnet wurden.

Bei einem Ausfall des Contact Centers werden die kommenden Anrufe über die verschiedenen UCD-Gruppen auf die angemeldeten Agenten verteilt.

Beispiel:

- UCD-Gruppe ABC werden die UCD-IDs 103, 104 und 105 zugeordnet. UCD-Gruppe XYZ wurden die UCD-IDs 108, 109 und 110 zugeordnet.
- Die Teilnehmer 123, 124 und 125 werden als Agenten mit den UCD-IDs 103, 104 und 105 konfiguriert. Die Teilnehmer 126, 127 und 128 werden als Agenten mit den UCD-IDs 108, 109 und 110 konfiguriert.
- Bei der Zuordnung von Agenten zu Warteschlangen müssen die Teilnehmer 123, 124 und 125 der Warteschlange ABC und die Teilnehmer 126, 127 und 128 der Warteschlange XYZ zugeordnet werden.



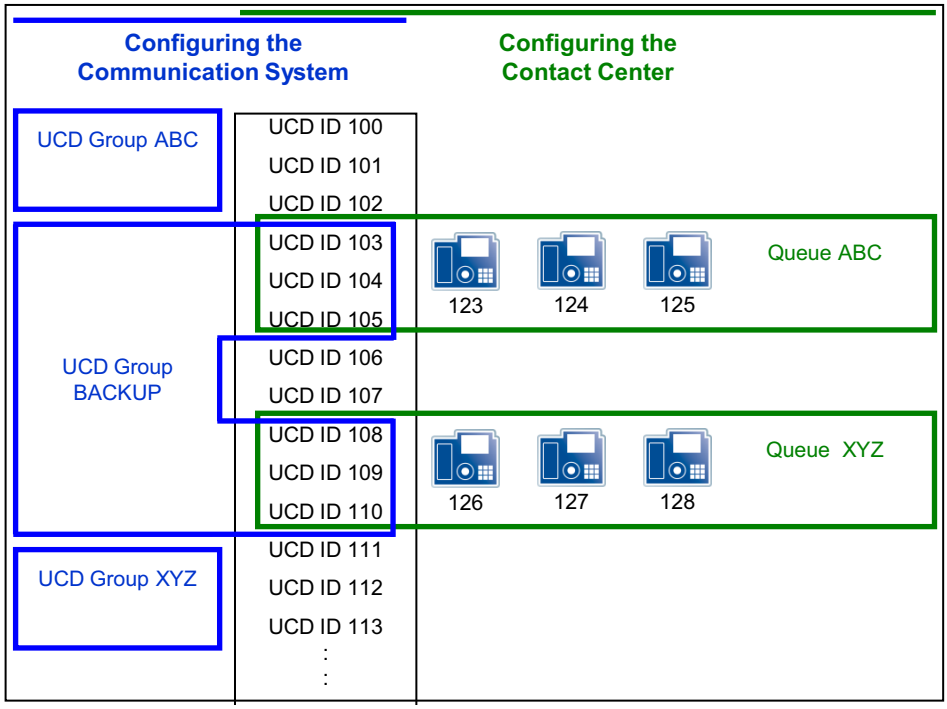
Basis-Rückfalllösung

In diesem Fall werden alle Agenten des Contact Centers anhand ihrer UCD-IDs nur der Backup-UCD-Gruppe zugeordnet. Durch die Zuordnung der entsprechenden Agenten werden diese UCD-IDs dann auch in den Warteschlangen des Contact Centers verwendet. Damit ist gewährleistet, dass bei Ausfall des Contact Centers sich die Agenten nicht mit einer anderen ID manuell an ihrem Telefon neu anmelden müssen. Für alle UCD-Gruppen des Kommunikationssystems wird diese Backup-UCD-Gruppe als Rufweiterschaltungsziel definiert.

Bei einem Ausfall des Contact Centers werden die kommenden Anrufe dann auf alle Agenten der Backup-UCD-Gruppe verteilt.

Beispiel:

- Den UCD-Gruppe ABC und XYZ wurden keine UCD-IDs zugeordnet. Der UCD-Gruppe BACKUP werden die UCD-IDs 103 bis 105 und 108 bis 110 zugeordnet.
- Die Teilnehmer 123, 124 und 125 werden als Agenten mit den UCD-IDs 103, 104 und 105 konfiguriert. Die Teilnehmer 126, 127 und 128 werden als Agenten mit den UCD-IDs 108, 109 und 110 konfiguriert.
- Bei der Zuordnung von Agenten zu Warteschlangen werden die Teilnehmer 123, 124 und 125 der Warteschlange ABC und die Teilnehmer 126, 127 und 128 der Warteschlange XYZ zugeordnet.



Kundenspezifische Rückfalllösung

In diesem Fall wird die kundenspezifische Konfiguration des Contact Centers über mehrere UCD-Gruppen nachgebildet.

Bei einem Ausfall des Contact Centers wird damit ein ähnliches Verhalten der Rückfalllösung erzielt.

Informationen zur Konfiguration einer Anrufverteilung über das Leistungsmerkmal "Uniform Call Distribution UCD" des Kommunikationssystems siehe *Anrufverteilung (UCD Uniform Call Distribution)*.

Wesentlicher Vorteil der kundenspezifischen Rückfalllösung ist die genaue Abbildung des Contact Centers auf die Rückfalllösung.

Nachteil der kundenspezifischen Rückfalllösung ist der hohe Konfigurationsaufwand. Darüber hinaus müssen alle Änderungen an der Contact Center-Konfiguration auch bei der Rückfalllösung nachgebildet werden, um ein ähnliches Verhalten der Anrufverteilung zu gewährleisten.

Wesentlicher Vorteil der Standard- und Basis-Rückfalllösung ist die einfache Konfiguration.

17.6 Konfiguration des Contact Centers

Bei der Konfiguration des Contact Centers sind zuerst die UCD-Gruppen zu definieren. Die Warteschlangen des Contact Centers sind Arbeitsgruppen, die auf den UCD-Gruppen des Kommunikationssystems basieren. Anschließend kann die eigentliche Konfiguration des Contact Centers (Zeitpläne, Warteschlangen usw.) durchgeführt werden.

Vor der Konfiguration des Contact Centers sind die Abläufe für die Anrufverteilung im Normal- und im Notfallbetrieb mit dem Kunden abzustimmen.

> ***INFO:*** Die Konfiguration des Contact Centers sollte erst erfolgen, nachdem die Einrichtung des Kommunikationssystems und der UC Suite vollständig abgeschlossen ist.

Werden Änderungen an der Konfiguration der UCD-Gruppen durchgeführt, muss anschließend die UC Suite über das Service Center des WBM neu gestartet werden.

Folgende Lizenzen sind Voraussetzung für den Betrieb eines Contact Centers:

- Eine entsprechende Anzahl Lizenzen für Agenten (myAgent)
- Contact-Center-Fax-Lizenz (für das Empfangen und Senden von Faxen), falls erforderlich
- Contact-Center-E-Mail-Lizenz (für das Empfangen und Senden von E-Mails), falls erforderlich

17.6.1 Beispiel für eine Contact-Center-Konfiguration

Anhand eines Beispiels wird das Funktionsprinzip des Contact Centers mit OpenScape Business dargestellt. Aufbau und Konfiguration des Beispiels basieren auf einem fiktiven Kundenszenario mit Contact-Center-Standardfunktionen.

Beispielszenario für ein Contact-Center

Die Firma XYZ betreibt ein Contact Center mit folgenden Rufnummern (Warteschlangen):

- Rufnummer 440 für den Bereich Service
- Rufnummer 444 für den Bereich Sales
- Rufnummer 456 für kostenlose Anrufe (Hotline). Anrufer erhalten eine Ansage und können anschließend durch Wahl der entsprechenden Ziffer den Bereich Service oder den Bereich Sales erreichen.

Das Contact Center besteht aus sechs Mitarbeitern (Agenten), wobei drei Mitarbeiter für den Bereich Service und drei Mitarbeiter für den Bereich Sales arbeiten.

Die Warteschlangen für die Bereiche Service und Sales sollen innerhalb der Geschäftszeiten von 09:00 Uhr bis 17:00 Uhr direkt erreichbar sein. Beide Warteschlangen verfügen über eine Faxbox und eine E-Mail-Adresse.

Sind alle Agenten im Gespräch oder nicht verfügbar, soll ein Anrufer darauf hingewiesen werden und Musik hören. Ist nach einer bestimmten Zeit kein Agent frei, kann ein Anrufer einen Rückrufwunsch hinterlassen oder durch Wahl einer bestimmten Ziffer zum Vermittlungsplatz gelangen. Wird keine Ziffer gewählt, soll der Anrufer automatisch in die Warteschlange zurückgeschaltet werden.

Außerhalb der Geschäftszeiten soll eine Ansage erfolgen, die eine Aufzeichnung mit Rückrufwunsch (Agentenrückruf) ermöglicht.

Während der Mittagspause von 12:00 Uhr bis 13:00 Uhr soll für die Warteschlangen der Bereiche Service und Sales eine Ansage erfolgen, die eine Aufzeichnung mit Rückrufwunsch ermöglicht.

Rückfalllösung (Fallback-Lösung) über Backup-UCD-Gruppe: Steht das Contact Center aufgrund von Problemen (Absturz, fehlende Verbindung oder ähnliches) nicht zur Verfügung, soll automatisch auf das Leistungsmerkmal "Uniform Call Distribution UCD" des Kommunikationssystems umgeschaltet werden. Dafür müssen alle Agenten des Contact Centers einer einzelnen Backup-UCD-Gruppe zugeordnet werden. Für alle UCD-Gruppen des Kommunikationssystems ist diese Backup-UCD-Gruppe als Rufweiterschaltungsziel zu definieren. Bei einem Ausfall des Contact Centers werden die kommenden Anrufe dann auf die Agenten der Backup-UCD-Gruppe verteilt.

Konfiguration des Beispielszenarios

Folgende Tätigkeiten sind für das Beispielszenario durchzuführen:

- Konfiguration von UCD-Gruppen
  Die Warteschlangen des Contact Centers sind Arbeitsgruppen, die auf den UCD-Gruppen des Kommunikationssystems basieren. Vor der eigentlichen Konfiguration des Contact Centers, müssen die UCD-Gruppen definiert werden.
  Für das vorliegende Beispiel des Contact Centers der Firma XYZ sind drei UCD-Gruppen (Service, Sales, Hotline) zu konfigurieren.
- Konfiguration der Rückfalllösung (Fallback-Lösung)
  Für das vorliegende Beispiel ist eine Backup-UCD-Gruppe zu konfigurieren und diese als Rufweiterschaltungsziel aller UCD-Gruppen des Kommunikationssystems zu definieren.
- Konfiguration von Teilnehmern als Agenten
  Für das vorliegende Beispiel sind sechs Teilnehmer als Agenten zu konfigurieren.
- Aufnehmen von individuellen Ansagen
  Für das vorliegende Beispiel sind verschiedene Ansagen aufzunehmen. Das sind beispielsweise Ansagen für den Fall, dass alle Agenten nicht verfügbar sind oder um einen Anrufer über mögliche Optionen (**Aktion nach Zifferneingabe ausführen**) zu informieren.
- Laden von individuellen Ansagen
  Für das vorliegende Beispiel sind die aufgenommenen Ansagen in das Kommunikationssystem zu laden.
- Definition von Zeitplänen
  Für jeden Zeitabschnitt innerhalb eines Zeitplans wird über Regeln (Call Control Vector CCV) definiert, wie kommende Anrufe an bestimmten Tagen und zu bestimmten Zeiten behandelt werden sollen.
  Für das vorliegende Beispiel ist ein Zeitplan (Standard Schedule XYZ) mit einer Regel für die Zeiten außerhalb der Geschäftszeiten und Ausnahmen für die Geschäftszeiten und die Mittagspause zu definieren. Darüber hinaus ist ein zweiter Zeitplan (Standard Schedule Hotline) mit einer Regel für kostenlose Anrufe (Hotline) zu definieren.

Zeitplan	Regel (CCV)	
Standard Schedule XYZ	Out Of The Office	Zeiten außerhalb der Geschäftszeiten
	Open	Geschäftszeit 08:00 Uhr bis 11:59 Uhr = Open1
		Geschäftszeit 13:00 Uhr bis 17:00 Uhr = Open2
	Lunch Break	Mittagspause 12:00 Uhr bis 12:59 Uhr
Standard Schedule Hotline	Hotline	24 Stunden

- Hinzufügen von drei Warteschlangen
  Für das vorliegende Beispiel ist eine Warteschlange für den Bereich Service und eine für den Bereich Sales zu konfigurieren. Eine weitere Warteschlange (Hotline) ist für kostenlose Anrufe zu konfigurieren.
- Agenten den Warteschlangen zuordnen
  Für das vorliegende Beispiel sind drei Agenten der Warteschlange Service und drei Agenten der Warteschlange Sales zuzuordnen.

Informationen über die Konfiguration aller Contact-Center-Funktionen finden Sie unter *Vorgehensweise bei der Konfiguration*.

17.6.1.1 Wie Sie UCD-Gruppen für das Beispiel-Contact-Center konfigurieren

Mit dem Wizard **Anrufverteilung** definieren Sie die drei UCD-Gruppen (Service, Sales, Hotline) mit den Rufnummern 440, 444 und 456 für das Beispiel-Contact-Center der Firma XYZ.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > User-Telefonie**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Anrufverteilung** zu starten. Es wird Ihnen die Liste aller möglichen UCD-Gruppen angezeigt.

4) Um eine UCD-Gruppe zu konfigurieren, klicken Sie in der Zeile der gewünschten UCD-Gruppe auf **Bearbeiten**.

5) Geben Sie im Feld **Rufnummer** die Rufnummer `440` der UCD-Gruppe Service ein.

6) Geben Sie im Feld **Durchwahlnummer** die Durchwahlnummer `440` der UCD-Gruppe Service ein.

7) Geben Sie im Feld **Name** den Namen `Service` ein.

8) Klicken Sie auf **OK & Weiter**. Das Fenster **Zuweisung der UCD-Agenten** wird angezeigt.

9) Klicken Sie auf **OK & Weiter**, da für die UCD-Gruppe Service keine UCD-IDs zugewiesen werden dürfen.

Da für das Beispiel-Contact-Center der Firma XYZ eine Rückfalllösung über eine Backup-UCD-Gruppe eingerichtet werden soll, dürfen den drei UCD-Gruppen Service, Sales und Hotline keine UCD-IDs zugewiesen werden.

10) Klicken Sie auf **OK & Weiter**. Das Fenster **Ansagen / Überlauf bearbeiten** wird angezeigt.

11) Klicken Sie auf **OK**, da die angezeigten Parameter für die Konfiguration der UCD-Gruppe nicht relevant sind.

12) Wiederholen Sie die Schritte 4 bis 11 für die UCD-Gruppe Sales mit der Rufnummer 444 und für die UCD-Gruppe Hotline mit der Rufnummer 456.

13) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

17.6.1.2 Wie Sie eine Rückfalllösung (Fallback-Lösung) für das Beispiel-Contact-Center konfigurieren

Mit dem Wizard **Anrufverteilung** konfigurieren Sie die Backup-UCD-Gruppe mit der Rufnummer 400 für das Beispiel-Contact-Center der Firma XYZ. Für das Beispiel werden die UCD-Agenten-IDs 101 bis 106 verwendet. Darüber hinaus definieren Sie die Backup-UCD-Gruppe als Rufweiterschaltungsziel aller UCD-Gruppen des Beispiel-Contact-Center der Firma XYZ.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > User-Telefonie**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Anrufverteilung** zu starten. Es wird Ihnen die Liste aller möglichen UCD-Gruppen angezeigt.

4) Um eine UCD-Gruppe zu konfigurieren, klicken Sie in der Zeile der gewünschten UCD-Gruppe auf **Bearbeiten**.

5) Geben Sie im Feld **Rufnummer** die Rufnummer `400` der UCD-Gruppe Backup ein.

6) Geben Sie im Feld **Durchwahlnummer** die Durchwahlnummer `400` der UCD-Gruppe Backup ein.

7) Geben Sie im Feld **Name** den Namen `Backup` ein.

8) Klicken Sie auf **OK & Weiter**. Das Fenster **Zuweisung der UCD-Agenten** wird angezeigt.

9) Markieren Sie die gewünschten UCD-Agenten-IDs in der **Auswahl** und weisen Sie diese der UCD-Gruppe Backup durch Klicken auf **Hinzufügen** zu.

10) Klicken Sie auf **OK & Weiter**. Das Fenster **Teilnehmer zuweisen** wird angezeigt.

11) Weisen Sie allen UCD-Agenten-IDs die gewünschten Teilnehmer zu.

12) Klicken Sie auf **OK & Weiter**. Das Fenster **Ansagen / Überlauf bearbeiten** wird angezeigt.

13) Klicken Sie auf **OK**, da die angezeigten Parameter für die Konfiguration der UCD-Gruppe Backup nicht relevant sind.

14) Um die neue UCD-Gruppe Backup als Rufweiterschaltungsziel der UCD-Gruppe Service zu konfigurieren, klicken Sie in der Zeile der UCD-Gruppe Service auf **Bearbeiten**.

15) Klicken Sie so oft auf **OK & Weiter**, bis das Fenster **Ansagen / Überlauf bearbeiten** angezeigt wird.

16) Wählen Sie in der Aufklappliste **Überlauf-Ziel** die UCD-Gruppe Backup mit der Rufnummer 400 als Rufweiterschaltungsziel aus.

17) Klicken Sie auf **OK**.

18) Wiederholen Sie die Schritte 14 bis 17, um die neue UCD-Gruppe Backup als Rufweiterschaltungsziel der UCD-Gruppen Sales und Hotline zu konfigurieren.

19) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

17.6.1.3 Wie Sie einen Teilnehmer als Agent für das Beispiel-Contact-Center konfigurieren

Mit dem Wizard **Benutzerverzeichnis** konfigurieren Sie Teilnehmer als Agenten für das Beispiel-Contact-Center der Firma XYZ. Für das Beispiel werden die Teilnehmer mit den Rufnummern 101 bis 106 als Agenten konfiguriert. Die Teilnehmer mit den Rufnummern 101 und 104 erhalten das Berechtigungs-Level **Supervisor**, die anderen Teilnehmer das Berechtigungs-Level **Agent**.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Benutzerverzeichnis** zu starten.

4) Markieren Sie den Teilnehmer mit der **Nebenstelle** 101 und klicken Sie auf **Bearbeiten**.

5) Klicken Sie im Menübaum auf **Persönliche Daten > Benutzerebene**.

6) Aktivieren Sie das Kontrollkästchen **Dauerverfügbarer Agent**. Der Agent bleibt auch dann für Anrufe, Faxe und E-Mails verfügbar, wenn er einen Anruf, ein Fax oder eine E-Mail nicht angenommen hat.

7) Wählen Sie in der Aufklappliste **Level** das Berechtigungs-Level **Supervisor** aus.

8) Klicken Sie auf **Speichern**.

9) Wiederholen Sie die Schritte 4 bis 8, um die Teilnehmer mit den Rufnummern 102 bis 106 als Agenten zu konfigurieren.

17.6.1.4 Wie Sie Ansagen für das Beispiel-Contact-Center aufnehmen

Mit dem Wizard **Aufzeichnungsgerät** können Sie Ansagen für das Beispiel-Contact-Center der Firma XYZ aufnehmen. Unter anderem ist für den Fall eine Ansage erforderlich, dass alle Agenten nicht erreichbar sind.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Aufzeichnungsgerät** zu starten.

4) Wählen Sie in der Aufklappliste **Nebenstelle** die Rufnummer des Telefons aus, über das die Aufnahme durchgeführt werden soll.

5) Klicken Sie auf **Beginnen**. Die ausgewählte Rufnummer wird angerufen.

6) Nehmen Sie den Hörer ab und geben Sie im Feld **Dateiname** den Namen für Ihre Ansage ein.

7) Klicken Sie auf **Aufzeichnen**, um die Aufnahme der Ansage zu starten.

8) Klicken Sie auf **Anhalten**, sobald Sie die Ansage komplett aufgesprochen haben.

9) Wenn Sie sich Ihre neue Ansage anhören möchten, klicken Sie auf **Wiedergeben**.

10) Klicken Sie auf **Schließen**, um die Ansage zu speichern.

INFO: Nach dem Aufnehmen und Speichern ist das Löschen einer Ansage nicht mehr möglich. Durch Verwenden des gleichen Dateinamens kann eine bereits gespeicherte Ansage aber überschrieben werden. Beispielsweise wird durch das Speichern

der Audiodatei `ansage1.wav` die bereits vorhandene Datei `ansage1.wav` überschrieben.

11) Wiederholen Sie die Schritte 3 bis 10, um weitere Ansagen für das Beispiel-Contact-Center der Firma XYZ aufzunehmen.

17.6.1.5 Wie Sie Ansagen für das Beispiel-Contact-Center laden

Mit dem Wizard **Datei-Upload** können Sie Ansagen für das Beispiel-Contact-Center der Firma XYZ laden.

Voraussetzungen

- Eine Audiodatei im wav-Format mit folgenden Eigenschaften liegt vor: Mono, Abtastrate 8 kHz, Abtastgröße 16 Bit, Framelänge 2.
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Datei-Upload** zu starten.

4) Klicken Sie auf die Registerkarte **Audiodatei laden**.

5) Wählen Sie in der Aufklappliste **Upload-Ziel** das Ziel **Vermittlungsplatz** aus.

6) Klicken Sie auf **Durchsuchen**, navigieren Sie zum gewünschten Ablageort der Audiodatei und klicken Sie auf **Öffnen**.

7) Klicken Sie auf **Upload**.

INFO: Nach dem Datei-Upload ist das Löschen einer Audiodatei nicht mehr möglich. Durch Verwenden des gleichen Dateinamens kann eine bereits geladene Audiodatei aber überschrieben werden. Beispielsweise wird durch das Laden der Audiodatei `ansage1.wav` die bereits vorhandene Datei `ansage1.wav` überschrieben.

8) Wiederholen Sie die Schritte 4 bis 7, um weitere Ansagen für das Beispiel-Contact-Center der Firma XYZ zu laden.

17.6.1.6 Wie Sie den Zeitplan Standard Schedule XYZ für das Beispiel-Contact-Center hinzufügen

Mit dem Wizard **Contact Center** definieren Sie den Zeitplan mit Regeln für die Pausen- und die Geschäftszeiten für das Beispiel-Contact-Center der Firma XYZ. Dazu ist ein Zeitplan (Standard Schedule XYZ) mit einer Regel für die Zeiten

außerhalb der Geschäftszeiten (Out Of The Office) und Ausnahmen für die Geschäftszeiten (08:00 Uhr bis 11:59 Uhr = Open1, 13:00 Uhr bis 17:00 Uhr = Open2) und die Mittagspause (12:00 Uhr bis 12:59 Uhr = Lunch Break) zu definieren.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

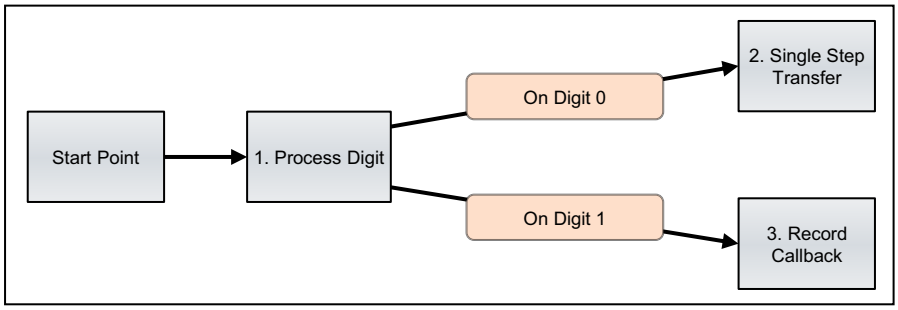
2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.

4) Klicken Sie auf **Zeitplan**. Alle bereits vorhandenen Zeitpläne werden angezeigt.

5) Klicken Sie auf **Hinzufügen**.

6) Definieren Sie die abgebildete Regel für Zeiten außerhalb der Geschäftszeiten.



Klicken Sie in der Liste der CCV-Tools auf eins der in der abgebildeten Regel enthaltenen CCV-Objekte und ziehen Sie es in den Regel-Editor. Geben Sie die nachfolgend genannten Eigenschaften in das sich öffnende Fenster des CCV-Objekts ein und bestätigen Sie diese durch Klicken auf **OK**. Wiederholen Sie den Vorgang für alle weiteren CCV-Objekte. Verbinden Sie die CCV-Objekte, indem Sie mit der rechten Maustaste auf das erste der beiden zu verbindenden CCV-Objekte klicken. Wählen Sie im Aufklappmenü über **Link To** das zweite der beiden zu verbindenden CCV-Objekte. Wiederholen Sie den Vorgang für alle weiteren zu verbindenden CCV-Objekte.

Eigenschaft	Wert
1. CCV-Objekt **Aktion nach Zifferneingabe ausführen**	
Wiedergabeliste	Audiodatei im wav-Format
Zeitüberschreitung bei Ziffern-eingabe	5
Beschreibung	Ansage: Mit Ziffer 0 können Sie ..., mit Ziffer 1 können Sie ...
2. CCV-Objekt **Einzelschritt-Übergabe**	

Eigenschaft		Wert
	Zielnebenstelle	100
	Beschreibung	Weiter zum Vermittlungsplatz
	Aktion nach Zifferneingabe	0
3. CCV-Objekt **Callback aufzeichnen**		
	Typ	Extensiver Rückruf
	Max. Nachrichtenlänge	20
	Beschreibung	Rückrufwunsch (Agentenrückruf)
	Aktion nach Zifferneingabe	1

Klicken Sie auf **Speichern ...**. Geben Sie `Out Of The Office` als Namen der Regel ein und klicken Sie anschließend auf **OK**. Ist die neue Regel fehlerhaft, ist kein Speichern möglich. Das oder die fehlerhaften CCV-Objekte werden im Regel-Editor rot markiert. Schließen Sie das Fenster, das das Speichern der Regel bestätigt.

Wählen Sie in der Aufklappliste **Standard-CCV** die Regel `Out Of The Office` aus.

7) Geben Sie im Feld **Name des Zeitplans** den Namen `Standard Schedule XYZ` ein.

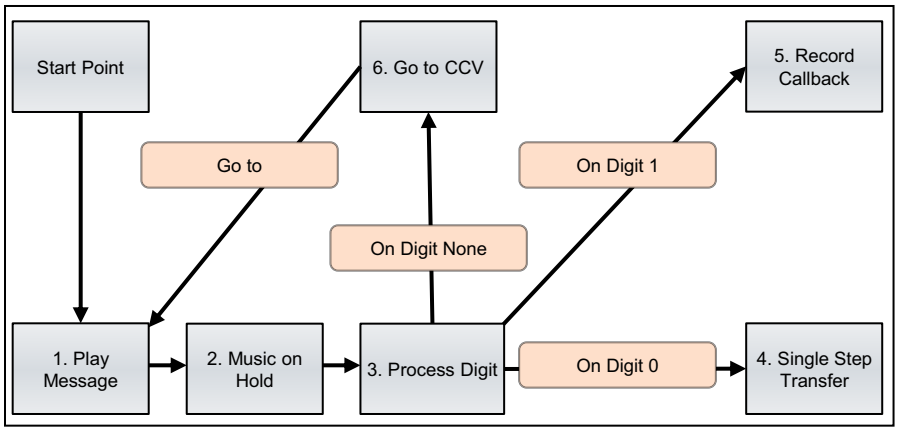
8) Klicken Sie auf **Zeitplan speichern** und anschließend auf **OK**.

9) Klicken Sie auf **Neu** und anschließend auf **Nein**.

10) Klicken Sie im Fensterbereich **Ausnahmen** auf **Hinzufügen**, um die erste Ausnahme für die Geschäftszeiten zu definieren.

11) Geben Sie im Feld **Beschreibung** `Open1` ein.

12) Definieren Sie die abgebildete Regel für die Geschäftszeiten.



Klicken Sie in der Liste der CCV-Tools auf eins der in der abgebildeten Regel enthaltenen CCV-Objekte und ziehen Sie es in den Regel-Editor. Geben Sie die nachfolgend genannten Eigenschaften in das sich öffnende Fenster des CCV-Objekts ein und bestätigen Sie diese durch Klicken auf **OK**. Wiederholen Sie den Vorgang für alle weiteren CCV-Objekte. Verbinden Sie die CCV-Objekte, indem Sie mit der rechten Maustaste auf das erste der beiden

zu verbindenden CCV-Objekte klicken. Wählen Sie im Aufklappmenü über **Link To** das zweite der beiden zu verbindenden CCV-Objekte. Wiederholen Sie den Vorgang für alle weiteren zu verbindenden CCV-Objekte.

Eigenschaft		Wert
1. CCV-Objekt **Nachricht abspielen**		
	Dateiname	Audiodatei im wav-Format
	Abbruchtasten	5
	Beschreibung	Ansage: Agenten nicht erreichbar
2. CCV-Objekt **Wartemusik**		
	Zeitwert	30
	Beschreibung	Wartemusik für 30 Sekunden
3. CCV-Objekt **Aktion nach Zifferneingabe ausführen**		
	Wiedergabeliste	Audiodatei im wav-Format
	Zeitüberschreitung bei Ziffern-eingabe	5
	Beschreibung	Ansage: Mit Ziffer 0 können Sie ..., mit Ziffer 1 können Sie ...
4. CCV-Objekt **Einzelschritt-Übergabe**		
	Zielnebenstelle	100
	Beschreibung	Weiter zum Vermittlungsplatz
	Aktion nach Zifferneingabe	0
5. CCV-Objekt **Callback aufzeichnen**		
	Typ	Extensiver Rückruf
	Max. Nachrichtenlänge	20
	Beschreibung	Rückrufwunsch (Agentenrückruf)
	Aktion nach Zifferneingabe	1
6. CCV-Objekt **Zu CCV**		
	Ziel CCV	1. Nachricht abspielen
	Beschreibung	Zurück zur Ansage

Klicken Sie auf **Speichern ...**. Geben Sie `Open` als Namen der Regel ein und klicken Sie anschließend auf **OK**. Schließen Sie das Fenster, das das Speichern der Regel bestätigt.

Wählen Sie in der Aufklappliste für die Ausnahme Open1 die Regel `Open` aus.

13) Definieren Sie, zu welcher Zeit die Ausnahme Open1 gelten soll:

Aktivieren Sie das Optionsfeld **Im Zeitbereich**. Wählen Sie in der Auswahlliste **Startzeit** `08:00` als Anfang und in der Auswahlliste **Endezeit** `11:59` als Ende des Tageszeitraums aus.

Klicken Sie auf **erfolgt täglich**. Wählen Sie im Fenster **Tage auswählen** die Wochentage aus, an denen die Regel gelten soll. Klicken Sie anschließend auf **Speichern**.

14) Klicken Sie auf das grüne Speichern-Symbol.

15) Klicken Sie im Fensterbereich **Ausnahmen** auf **Hinzufügen**, um die zweite Ausnahme für die Geschäftszeiten zu definieren.

16) Geben Sie im Feld **Beschreibung** `Open2` ein.

17) Wählen Sie in der Aufklappliste für die Ausnahme Open2 die Regel `Open` aus.

18) Definieren Sie, zu welcher Zeit die Ausnahme Open2 gelten soll:

Aktivieren Sie das Optionsfeld **Im Zeitbereich**. Wählen Sie in der Auswahlliste **Startzeit** `13:00` als Anfang und in der Auswahlliste **Endezeit** `17:00` als Ende des Tageszeitraums aus.

Klicken Sie auf **erfolgt täglich**. Wählen Sie im Fenster **Tage auswählen** die Wochentage aus, an denen die Regel gelten soll. Klicken Sie anschließend auf **Speichern**.

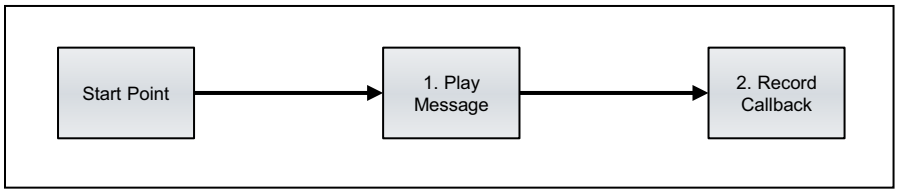
19) Klicken Sie auf das grüne Speichern-Symbol.

20) Klicken Sie auf **Neu** und anschließend auf **Nein**.

21) Klicken Sie im Fensterbereich **Ausnahmen** auf **Hinzufügen**, um die Ausnahme für die Mittagspause zu definieren.

22) Geben Sie im Feld **Beschreibung** `Lunch Break` ein.

23) Definieren Sie die abgebildete Regel für die Mittagspause.



Klicken Sie in der Liste der CCV-Tools auf eins der in der abgebildeten Regel enthaltenen CCV-Objekte und ziehen Sie es in den Regel-Editor. Geben Sie die nachfolgend genannten Eigenschaften in das sich öffnende Fenster des CCV-Objekts ein und bestätigen Sie diese durch Klicken auf **OK**. Wiederholen Sie den Vorgang für alle weiteren CCV-Objekte. Verbinden Sie die CCV-Objekte, indem Sie mit der rechten Maustaste auf das erste der beiden zu verbindenden CCV-Objekte klicken. Wählen Sie im Aufklappmenü über **Link To** das zweite der beiden zu verbindenden CCV-Objekte. Wiederholen Sie den Vorgang für alle weiteren zu verbindenden CCV-Objekte.

Eigenschaft		Wert
1. CCV-Objekt **Nachricht abspielen**		
	Dateiname	Audiodatei im wav-Format
	Abbruchtasten	Service auswählen
	Beschreibung	Ansage: Agenten nicht erreichbar
2. CCV-Objekt **Callback aufzeichnen**		

Eigenschaft	Wert
Typ	Extensiver Rückruf
Max. Nachrichtenlänge	20
Beschreibung	Rückrufwunsch (Agentenrückruf)
Aktion nach Zifferneingabe	1

Klicken Sie auf **Speichern ...**. Geben Sie `Lunch Break` als Namen der Regel ein und klicken Sie anschließend auf **OK**. Schließen Sie das Fenster, das das Speichern der Regel bestätigt.

Wählen Sie in der Aufklappliste für die Ausnahme Lunch Break die Regel `Lunch Break` aus.

24) Definieren Sie, zu welcher Zeit die Ausnahme Lunch Break gelten soll:

Aktivieren Sie das Optionsfeld **Im Zeitbereich**. Wählen Sie in der Auswahlliste **Startzeit** `12:00` als Anfang und in der Auswahlliste **Endezeit** `12:59` als Ende des Tageszeitraums aus.

Klicken Sie auf **erfolgt täglich**. Wählen Sie im Fenster **Tage auswählen** die Wochentage aus, an denen die Regel gelten soll. Klicken Sie anschließend auf **Speichern**.

25) Klicken Sie auf das grüne Speichern-Symbol.

26) Wenn Sie testen möchten, welche Regel (CCV) des Zeitplans an einem bestimmten Zeitpunkt ausgeführt wird, klicken Sie auf **Zeitplan testen**. Wählen Sie in der Aufklappliste **Datum** den gewünschten Tag und in der Auswahlliste **Zeit** die gewünschte Uhrzeit aus. Klicken Sie auf **Zeitplan testen**. Anschließend wird angezeigt, welche Regel (CCV) an diesem Tag und zu dieser Uhrzeit aktiv ist. Klicken Sie auf **Schließen**, um das Fenster **Zeitplan testen** zu schließen.

27) Klicken Sie auf **Zeitplan speichern** und anschließend auf **OK**.

28) Schließen Sie das Fenster und bestätigen Sie das Schließen mit **Ja**.

17.6.1.7 Wie Sie den Zeitplan Standard Schedule Hotline für das Beispiel-Contact-Center hinzufügen

Mit dem Wizard **Contact Center** definieren Sie den Zeitplan mit einer Regel für kostenlose Anrufe (Hotline) für das Beispiel-Contact-Center der Firma XYZ.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

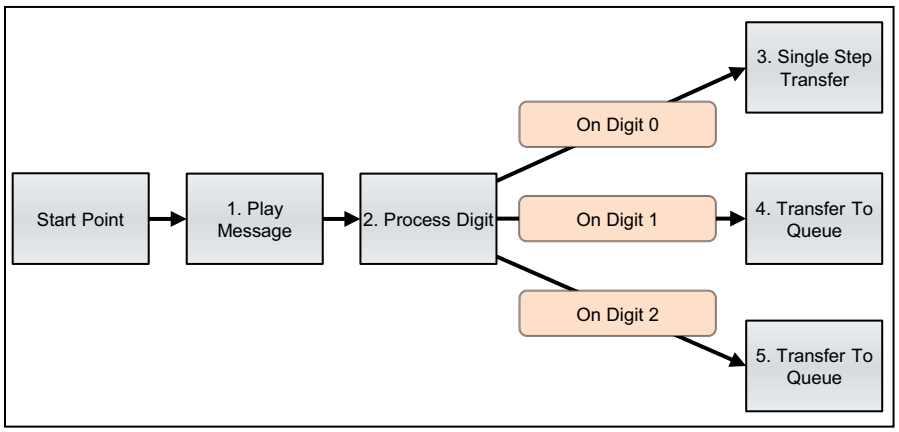
2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.

4) Klicken Sie auf **Zeitplan**. Alle bereits vorhandenen Zeitpläne werden angezeigt.

5) Klicken Sie auf **Hinzufügen**.

6) Definieren Sie die abgebildete Regel für kostenlose Anrufe (Hotline).



Klicken Sie in der Liste der CCV-Tools auf eins der in der abgebildeten Regel enthaltenen CCV-Objekte und ziehen Sie es in den Regel-Editor. Geben Sie die nachfolgend genannten Eigenschaften in das sich öffnende Fenster des CCV-Objekts ein und bestätigen Sie diese durch Klicken auf **OK**. Wiederholen Sie den Vorgang für alle weiteren CCV-Objekte. Verbinden Sie die CCV-Objekte, indem Sie mit der rechten Maustaste auf das erste der beiden zu verbindenden CCV-Objekte klicken. Wählen Sie im Aufklappmenü über **Link To** das zweite der beiden zu verbindenden CCV-Objekte. Wiederholen Sie den Vorgang für alle weiteren zu verbindenden CCV-Objekte.

Eigenschaft		Wert
1. CCV-Objekt **Nachricht abspielen**		
	Dateiname	Audiodatei im wav-Format
	Abbruchtasten	5
	Beschreibung	Ansage: Begrüßung
2. CCV-Objekt **Aktion nach Zifferneingabe ausführen**		
	Wiedergabeliste	Audiodatei im wav-Format
	Zeitüberschreitung bei Ziffern-eingabe	5
	Beschreibung	Ansage: Mit Ziffer 0 können Sie ..., mit Ziffer 1 können Sie ...
3. CCV-Objekt **Einzelschritt-Übergabe**		
	Zielnebenstelle	100
	Beschreibung	Weiter zum Vermittlungsplatz
	Aktion nach Zifferneingabe	0
4. CCV-Objekt **An Warteschlange übergeben**		

Eigenschaft		Wert
	Warteschlange	440
	Beschreibung	Weiter zur Warteschlange Service
	Aktion nach Zifferneingabe	1
5. CCV-Objekt **An Warteschlange übergeben**		
	Warteschlange	444
	Beschreibung	Weiter zur Warteschlange Sales
	Aktion nach Zifferneingabe	2

Klicken Sie auf **Speichern ...**. Geben Sie `Hotline` als Namen der Regel ein und klicken Sie anschließend auf **OK**. Ist die neue Regel fehlerhaft, ist kein Speichern möglich. Das oder die fehlerhaften CCV-Objekte werden im Regel-Editor rot markiert. Schließen Sie das Fenster, das das Speichern der Regel bestätigt.

Wählen Sie in der Aufklappliste **Standard-CCV** die Regel `Hotline` aus.

7) Geben Sie im Feld **Name des Zeitplans** den Namen `Standard Schedule Hotline` ein.

8) Klicken Sie auf **Zeitplan speichern** und anschließend auf **OK**.

9) Schließen Sie das Fenster und bestätigen Sie das Schließen mit **Ja**.

17.6.1.8 Wie Sie Warteschlangen für das Beispiel-Contact-Center hinzufügen

Mit dem Wizard **Contact Center** konfigurieren Sie die Warteschlangen für das Beispiel-Contact-Center der Firma XYZ. Für das Beispiel ist eine Warteschlange für den Bereich Service (Rufnummer 440) und eine für den Bereich Sales (Rufnummer 444) zu konfigurieren. Eine weitere Warteschlange (Hotline, Rufnummer 456) ist für kostenlose Anrufe zu konfigurieren.

Voraussetzungen

- Die UCD-Gruppen **Service**, **Sales** und **Hotline** für das Beispiel-Contact-Center wurden eingerichtet.
- Die Zeitpläne **Standard Schedule XYZ** und **Standard Schedule Hotline** für das Beispiel-Contact-Center wurden eingerichtet.
- Mindestens ein E-Mail-Account für den E-Mail-Empfang steht zur Verfügung.
- Der E-Mail-Versand im Kommunikationssystem ist konfiguriert.
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.

4) Klicken Sie auf **Warteschlange**.

5) Klicken Sie auf **Hinzufügen**.

6) Klicken Sie auf die Registerkarte **Allgemeine Einstellungen**.

7) Geben Sie im Feld **Name der Warteschlange** den Namen `Service` ein.

8) Wählen Sie in der Aufklappliste **Warteschlange aktiv** den Eintrag **Aktiv** aus.

9) Geben Sie im Feld **Gruppennummer** die Rufnummer `440` ein.

10) Wählen Sie in der Aufklappliste **Telefonanlage** den Eintrag **CSP** aus.

11) Wählen Sie in der Aufklappliste **Zeitplan** den Eintag **Standard Schedule XYZ** aus.

12) Geben Sie im Feld **Anzahl Warteschlangen-Alarme** beispielsweise `20` ein.

Sind mehr als 20 wartende Anrufe in der Warteschlange, wechselt das Warteschlangensymbol bei den Agenten von grün auf orange.

13) Geben Sie im Feld **Zeit Warteschlangen-Alarm** beispielsweise `300` ein.

Sobald die Wartezeit eines Anrufs in der Warteschlange 300 Sekunden übersteigt, wechselt der betreffende Eintrag in der Liste der Contact-Center-Anrufe bei den Agenten auf rot.

14) Geben Sie im Feld **Zeitüberschreitung für entgangene Anrufe** beispielsweise `100` ein, damit ein nicht angenommener Anruf nach 100 Sekunden zum nächsten freien Agenten weitergeleitet wird.

15) Geben Sie im Feld **Schwellwert für abgebrochene Anrufe** beispielsweise `120` ein. Damit werden Anrufe in die Statistik (in einen Bericht) aufgenommen, die nach 120 Sekunden abgebrochen werden.

16) Aktivieren Sie das Kontrollkästchen **Popup-Fenster aktiviert**, damit bei kommenden Anrufen in myAgent ein PopUp-Fenster zur Anzeige und Eingabe von Kundendaten erscheint.

17) Aktivieren Sie die Option **Keine Nachbearbeitung**.

18) Klicken Sie auf die Registerkarte **Warteschlangen-Pilots**.

19) Aktivieren Sie im Bereich **Pilots für eingehende Faxnachrichten** das oder die Kontrollkästchen des oder der gewünschten Pilots (Rufnummer(n)), damit Faxe in die Warteschlange übernommen werden.

Faxe an diese Rufnummer(n) werden in die Warteschlange übernommen und wie kommende Anrufe behandelt.

20) Wählen Sie eine der folgenden Möglichkeiten im Bereich **Dienst für eingehende E-Mails**, damit E-Mails in die Warteschlange übernommen werden:

- Wenn Sie eine neue E-Mail-Adresse einrichten möchten, klicken Sie auf **Neue E-Mail**. Das Fenster **Warteschlangen-E-Mail-Pilot bearbeiten** wird angezeigt.

  Geben Sie im Feld **Server** die Bezeichnung des E-Mail-Servers ein, der für das Abholen der E-Mails verwendet werden soll (zum Beispiel `pop3.web.de`).

  Geben Sie im Feld **Port** die Portnummer des E-Mail-Servers ein (zum Beispiel `110`, die Standardportnummer für POP3).

  Geben Sie im Feld **Benutzername** und im Feld **Kennwort** die Zugangsdaten für den E-Mail-Server ein.

  Wählen Sie aus, ob der E-Mail-Versand über eine SSL (Secure Socket Layer)-Verbindung erfolgen soll: Wenn Sie eine SSL-Verbindung nutzen möchten, aktivieren Sie das Kontrollkästchen **Verwendet SSL-Verbindung** (Dadurch ändert sich gegebenenfalls die Portnummer des E-Mail-Servers. Standardportnummer für POP3 via SSL = 995). Wenn Sie keine SSL-Verbindung nutzen möchten, deaktivieren Sie das Kontrollkästchen **Verwendet SSL-Verbindung**.

  Klicken Sie auf **OK**. Die neue E-Mail-Adresse wird anschließend im Bereich **Dienst für eingehende E-Mails** angezeigt.

- Wenn Sie eine bestehende E-Mail-Adresse ändern möchten, markieren Sie die gewünschte E-Mail-Adresse und klicken Sie auf **E-Mail bearbeiten**. Das Fenster **Warteschlangen-E-Mail-Pilot bearbeiten** wird angezeigt.

  Ändern Sie die gewünschten Parameter und klicken Sie anschließend auf **OK**.

- Wenn Sie eine bestehende E-Mail-Adresse löschen möchten, markieren Sie die gewünschte E-Mail-Adresse und klicken Sie auf **E-Mail entfernen**.

21) Klicken Sie auf die Registerkarte **Verschiedenes**.

22) Geben Sie im Feld **Absender-E-Mail-Adresse** die E-Mail-Adresse ein, die beim Versenden einer E-Mail durch einen Agenten beim Empfänger angezeigt werden soll.

23) Klicken Sie auf **Speichern**.

24) Wiederholen Sie die Schritte 5 bis 23, um die Warteschlange Sales zu konfigurieren. Wiederholen Sie die Schritte 5 bis 17 und 23, um die Warteschlange Hotline zu konfigurieren.

17.6.1.9 Wie Sie Agenten den Warteschlangen des Beispiel-Contact-Centers zuordnen

Mit dem Wizard **Contact Center** ordnen Sie die Agenten den Warteschlangen für das Beispiel-Contact-Center der Firma XYZ zu. Für das Beispiel sind drei Agenten der Warteschlange Service und drei Agenten der Warteschlange Sales zuzuordnen.

Voraussetzungen

- Die Warteschlangen **Service** und **Sales** für das Beispiel-Contact-Center wurden eingerichtet.
- Sechs Agenten für das Beispiel-Contact-Center wurden konfiguriert.
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.

4) Klicken Sie auf **Warteschlangen-Bindungen**. Die Warteschlangen **Service** und **Sales** und sechs Agenten werden angezeigt.

5) Klicken Sie auf die Warteschlange, der Sie einen Agenten zuordnen möchten. Alle bereits zugeordneten Agenten werden angezeigt.

6) Ziehen Sie den ersten Agenten auf die Warteschlangen **Service**. Anschließend wird das Fenster **Agentenzuweisung für Warteschlange** angezeigt.

7) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn der Agent Anrufe unabhängig von der Auslastung der Warteschlange **Service** erhalten soll, aktivieren Sie das Optionsfeld **Hauptagent**.
- Wenn der Agent Anrufe nur bei Überlauf der Warteschlange **Service** erhalten soll, aktivieren Sie das Optionsfeld **Agent bei Überlauf**.

8) Wenn Sie **Agent bei Überlauf** gewählt haben:

a) Geben Sie im Feld **Überlauf nach Sekunden in Wartes.** die Zeit ein, nach deren Ablauf ein Anruf an einen Agenten bei Überlauf weitergeleitet werden soll.

b) Geben Sie im Feld **Überlauf nach Anrufen in Wartes.** die Maximalzahl von Anrufen ein. Ein Agent bei Überlauf erhält Anrufe, die über diese Maximalzahl hinausgehen.

9) Stellen Sie einen Prozentwert für das **Fähigkeits-Level** des Agenten ein.

Durch das Fähigkeits-Level steuern Sie die Verteilung der Anrufe auf die Agenten in der Warteschlange **Service**. Agenten mit höherem Fähigkeits-Level werden bei der Anrufverteilung bevorzugt. Haben alle Agenten das gleiche Fähigkeits-Level, erhält der am längsten freie Agent den Anruf.

10) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn der Agent Rückrufwünsche in Form von Sprachnachrichten erhalten soll, aktivieren Sie das Kontrollkästchen **Agentenrückruf aktivieren**.
- Wenn der Agent keine Rückrufwünsche erhalten soll, deaktivieren Sie das Kontrollkästchen **Agentenrückruf aktivieren**.

11) Geben Sie im Feld **Nachbearbeitung** die automatische Nachbearbeitungszeit in Sekunden für den Agenten in der Warteschlange **Service** ein.

12) Klicken Sie auf **OK**.

13) Wiederholen Sie die Schritte 5 bis 12, um alle Agenten den Warteschlangen des Beispiel-Contact-Centers zuzuordnen.

17.6.2 Vorgehensweise bei der Konfiguration

Hier erhalten Sie einen Überblick über die bei der Konfiguration des Contact Centers durchzuführenden Tätigkeiten.

- Konfiguration der UCD-Gruppen
  Die Warteschlangen des Contact Centers sind Arbeitsgruppen, die auf den UCD-Gruppen des Kommunikationssystems basieren. Vor der eigentlichen Konfiguration des Contact Centers, müssen die UCD-Gruppen definiert werden.
- Konfiguration einer Rückfalllösung (Fallback-Lösung)
  Steht das Contact Center aufgrund von Problemen (Absturz, fehlende Verbindung oder ähnliches) nicht zur Verfügung, wird automatisch auf das Leistungsmerkmal "Uniform Call Distribution UCD" des Kommunikationssystems umgeschaltet. Das Leistungsmerkmal dient damit als Rückfalllösung für das Contact Center (siehe *Rückfalllösung (Fallback-Lösung)*).
- Konfiguration von Teilnehmern als Agenten
- Aufnehmen von individuellen Ansagen für das Contact Center
- Laden von individuellen Ansagen für das Contact Center
- Hinzufügen von Zeitplänen
- Hinzufügen von Warteschlangen
- Festlegen von Sollwerten für den Servicegrad
- Festlegen der VIP-Anruferpriorität
- Bearbeiten der VIP-Rufliste
- Festlegen von bevorzugten Agenten
- Hinzufügen von Contact Center-Pausen
- Hinzufügen von Nachbearbeitungscodes
- Zuordnen von Agenten zu Warteschlangen

17.6.2.1 Wie Sie UCD-Gruppen für das Contact Center konfigurieren

Mit dem Wizard **Anrufverteilung** können Sie UCD-Gruppen für das Contact Center konfigurieren.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards > User-Telefonie**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Anrufverteilung** zu starten. Es wird Ihnen die Liste aller möglichen UCD-Gruppen angezeigt.
4) Um eine UCD-Gruppe zu konfigurieren, klicken Sie in der Zeile der gewünschten UCD-Gruppe auf **Bearbeiten**.
5) Geben Sie im Feld **Rufnummer** die Rufnummer der UCD-Gruppe ein.
6) Geben Sie im Feld **Durchwahlnummer** die Durchwahlnummer der UCD-Gruppe ein.
7) Geben Sie im Feld **Name** den Namen der UCD-Gruppe ein.
8) Klicken Sie auf **OK & Weiter**. Das Fenster **Zuweisung der UCD-Agenten** wird angezeigt.
9) Markieren Sie die gewünschten UCD-Agenten-IDs in der **Auswahl** und weisen Sie diese der UCD-Gruppe durch Klicken auf **Hinzufügen** zu.
10) Klicken Sie auf **OK & Weiter**. Das Fenster **Teilnehmer zuweisen** wird angezeigt.
11) Weisen Sie allen UCD-Agenten-IDs die gewünschten Teilnehmer zu.
12) Klicken Sie auf **OK & Weiter**. Das Fenster **Ansagen / Überlauf bearbeiten** wird angezeigt.
13) Klicken Sie auf **OK**, da die angezeigten Parameter für die Konfiguration der UCD-Gruppe nicht relevant sind.
14) Wenn Sie weitere UCD-Gruppen für das Contact Center konfigurieren möchten, wiederholen Sie die Schritte 4 bis 13.
15) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

17.6.2.2 Wie Sie einen Teilnehmer als Agent konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Benutzerverzeichnis** zu starten.
4) Markieren Sie den gewünschten Teilnehmer im Benutzerverzeichnis und klicken Sie auf **Bearbeiten**.
5) Klicken Sie im Menübaum auf **Persönliche Daten > Benutzerebene**.

6) Wählen Sie eine der folgenden Möglichkeiten:

Wenn der Agent dauerverfügbar sein soll, aktivieren Sie das Kontrollkästchen **Dauerverfügbarer Agent**. Der Agent bleibt auch dann für Anrufe, Faxe und E-Mails verfügbar, wenn er einen Anruf, ein Fax oder eine E-Mail nicht angenommen hat.

Wenn der Agent nicht dauerverfügbar sein soll, deaktivieren Sie das Kontrollkästchen **Dauerverfügbarer Agent**. Der Agent erhält den Zustand nicht verfügbar, wenn er einen Anruf, ein Fax oder eine E-Mail nicht angenommen hat.

7) Wählen Sie in der Aufklappliste **Level** das Berechtigungs-Level aus.

8) Klicken Sie auf **Speichern**.

9) Wenn Sie einen weiteren Teilnehmer als Agent konfigurieren möchten, wiederholen Sie Schritt 4 bis Schritt 8.

17.6.2.3 Wie Sie eine individuelle Ansage für das Contact Center aufnehmen

Mit dem Wizard **Aufzeichnungsgerät** können Sie individuelle Ansagen für das Contact Center aufnehmen.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Aufzeichnungsgerät** zu starten.

4) Wählen Sie in der Aufklappliste **Nebenstelle** die Rufnummer des Telefons aus, über das die Aufnahme durchgeführt werden soll.

5) Klicken Sie auf **Beginnen**. Die ausgewählte Rufnummer wird angerufen.

6) Nehmen Sie den Hörer ab und geben Sie im Feld **Dateiname** den Namen für Ihre Ansage ein.

7) Klicken Sie auf **Aufzeichnen**, um die Aufnahme der Ansage zu starten.

8) Klicken Sie auf **Anhalten**, sobald Sie die Ansage komplett aufgesprochen haben.

9) Wenn Sie sich Ihre neue Ansage anhören möchten, klicken Sie auf **Wiedergeben**.

10) Klicken Sie auf **Schließen**, um die Ansage zu speichern.

INFO: Nach dem Aufnehmen und Speichern ist das Löschen einer Ansage nicht mehr möglich. Durch Verwenden des gleichen Dateinamens kann eine bereits gespeicherte Ansage aber

überschrieben werden. Beispielsweise wird durch das Speichern der Audiodatei `ansage1.wav` die bereits vorhandene Datei `ansage1.wav` überschrieben.

17.6.2.4 Wie Sie eine individuelle Ansage für das Contact Center laden

Mit dem Wizard **Datei-Upload** können Sie individuelle Ansagen für das Contact Center laden.

Voraussetzungen

- Eine Audiodatei im wav-Format mit folgenden Eigenschaften liegt vor: Mono, Abtastrate 8 kHz, Abtastgröße 16 Bit, Framelänge 2.
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Datei-Upload** zu starten.
4) Klicken Sie auf die Registerkarte **Audiodatei laden**.
5) Wählen Sie in der Aufklappliste **Upload-Ziel** das Ziel **Vermittlungsplatz** aus.
6) Klicken Sie auf **Durchsuchen**, navigieren Sie zum Ablageort der gewünschten Audiodatei und klicken Sie auf **Öffnen**.
7) Klicken Sie auf **Upload**.

INFO: Nach dem Datei-Upload ist das Löschen einer Audiodatei nicht mehr möglich. Durch Verwenden des gleichen Dateinamens kann eine bereits geladene Audiodatei aber überschrieben werden. Beispielsweise wird durch das Laden der Audiodatei `ansage1.wav` die bereits vorhandene Datei `ansage1.wav` überschrieben.

17.6.2.5 Wie Sie einen Zeitplan hinzufügen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.

4) Klicken Sie auf **Zeitplan**. Alle bereits vorhandenen Zeitpläne werden angezeigt.

5) Klicken Sie auf **Hinzufügen**.

6) Wählen Sie für die Auswahl der Regel (CCV) eine der folgenden Möglichkeiten aus:

- Wenn Sie dem Zeitplan eine bereits definierte Regel zuweisen möchten, wählen Sie in der Aufklappliste **Standard-CCV** die gewünschte Regel aus.
- Wenn Sie dem Zeitplan eine neue, noch nicht definierte Regel zuweisen möchten, gehen Sie wie folgt vor:

  Klicken Sie in der Liste der CCV-Tools auf das gewünschte CCV-Objekt und ziehen Sie es in den Regel-Editor. Geben Sie die gewünschten Eigenschaften in das sich öffnende Fenster des CCV-Objekts ein und bestätigen Sie diese durch Klicken auf **OK**. Falls erforderlich, ziehen Sie weitere CCV-Objekte in den Regel-Editor und definieren Sie deren Eigenschaften. Um zwei CCV-Objekte zu verbinden, klicken Sie mit der rechten Maustaste auf das erste der beiden zu verbindenden CCV-Objekte. Wählen Sie im Aufklappmenü über **Link To** das zweite der beiden zu verbindenden CCV-Objekte.

  Wenn Sie ein CCV-Objekt aus dem Regel-Editor löschen möchten, klicken Sie mit der rechten Maustaste auf das betreffende CCV-Objekt und wählen Sie im Aufklappmenü **Entfernen**.

  Klicken Sie auf **Speichern ...**. Geben Sie den Namen der neuen Regel ein und klicken Sie anschließend auf **OK**. Schließen Sie das Fenster, das das Speichern der Regel bestätigt. Ist die neue Regel fehlerhaft, ist kein Speichern möglich. Das oder die fehlerhaften CCV-Objekte werden im Regel-Editor rot markiert.

  Wählen Sie in der Aufklappliste **Standard-CCV** die neue, soeben gespeicherte Regel aus.
- Wenn Sie dem Zeitplan eine neue Regel zuweisen möchten, die auf einer bereits definierten Regel basiert, gehen Sie wie folgt vor:

  Wählen Sie in der Aufklappliste **Standard-CCV** die gewünschte Regel aus und klicken Sie auf **Bearbeiten**. Die Regel wird im Regel-Editor angezeigt. Ändern Sie die Regel.

  Klicken Sie auf **Speichern ...**. Geben Sie den Namen der neuen Regel ein und klicken Sie anschließend auf **OK**. Schließen Sie das Fenster, das das Speichern der Regel bestätigt. Ist die neue Regel fehlerhaft, ist kein Speichern möglich. Das oder die fehlerhaften CCV-Objekte werden im Regel-Editor rot markiert.

  Wählen Sie in der Aufklappliste **Standard-CCV** die neue, soeben gespeicherte Regel aus.

7) Wenn Sie die Regel ausdrucken oder per E-Mail verschicken möchten, können Sie die Regel als PDF-Datei speichern. Klicken Sie dazu auf **Druckfähiges Bild speichern**. Das Speichern-Fenster erscheint.

Geben Sie den Namen der Datei ein und wählen Sie das Verzeichnis aus, in dem die Datei gespeichert werden soll. Klicken Sie auf **Speichern**.

8) Geben Sie im Feld **Name des Zeitplans** den Namen des neuen Zeitplans ein.

9) Klicken Sie auf **Zeitplan speichern** und anschließend auf **OK**.

10) Wenn Sie einem bestimmten Zeitraum innerhalb des Zeitplans eine andere Regel (CCV) zuweisen möchten, klicken Sie im Fensterbereich **Ausnahmen** auf **Hinzufügen**. Anschließend werden die Felder für diese Ausnahme angezeigt.

11) Geben Sie im Feld **Beschreibung** den Namen der Ausnahme ein.

12) Wählen Sie für die Auswahl der Regel (CCV) eine der folgenden Möglichkeiten aus:

- Wenn Sie dem Zeitraum innerhalb des Zeitplans eine bereits definierte Regel zuweisen möchten, wählen Sie in der Aufklappliste für diese Ausnahme die gewünschte Regel aus.
- Wenn Sie dem Zeitraum innerhalb des Zeitplans eine neue, noch nicht definierte Regel zuweisen möchten, gehen Sie wie folgt vor:

  Klicken Sie auf **Neu** und anschließend auf **Nein**.

  Klicken Sie in der Liste der CCV-Tools auf das gewünschte CCV-Objekt und ziehen Sie es in den Regel-Editor. Geben Sie die gewünschten Eigenschaften in das sich öffnende Fenster des CCV-Objekts ein und bestätigen Sie diese durch Klicken auf **OK**. Falls erforderlich, ziehen Sie weitere CCV-Objekte in den Regel-Editor und definieren Sie deren Eigenschaften. Um zwei CCV-Objekte zu verbinden, klicken Sie mit der rechten Maustaste auf das erste der beiden zu verbindenden CCV-Objekte. Wählen Sie im Aufklappmenü über **Link To** das zweite der beiden zu verbindenden CCV-Objekte.

  Wenn Sie ein CCV-Objekt aus dem Regel-Editor löschen möchten, klicken Sie mit der rechten Maustaste auf das betreffende CCV-Objekt und wählen Sie im Aufklappmenü **Entfernen**.

  Klicken Sie auf **Speichern ...**. Geben Sie den Namen der neuen Regel ein und klicken Sie anschließend auf **OK**. Schließen Sie das Fenster, das das Speichern der Regel bestätigt. Ist die neue Regel fehlerhaft, ist kein Speichern möglich. Das oder die fehlerhaften CCV-Objekte werden im Regel-Editor rot markiert.

  Wählen Sie in der Aufklappliste für diese Ausnahme die neue, soeben gespeicherte Regel aus.

- Wenn Sie dem Zeitraum innerhalb des Zeitplans eine neue Regel zuweisen möchten, die auf einer bereits definierten Regel basiert, gehen Sie wie folgt vor:

  Wählen Sie in der Aufklappliste für diese Ausnahme die gewünschte Regel aus und klicken Sie auf **Bearbeiten**. Die Regel wird im Regel-Editor angezeigt. Ändern Sie die Regel.

  Klicken Sie auf **Speichern ...**. Geben Sie den Namen der neuen Regel ein und klicken Sie anschließend auf **OK**. Schließen Sie das Fenster, das das Speichern der Regel bestätigt. Ist die neue Regel fehlerhaft, ist kein Speichern möglich. Das oder die fehlerhaften CCV-Objekte werden im Regel-Editor rot markiert.

  Wählen Sie in der Aufklappliste für diese Ausnahme die neue, soeben gespeicherte Regel aus.

13) Wählen Sie eine der folgenden Möglichkeiten, um festzulegen, zu welcher Zeit die Ausnahme gelten soll:

- Wenn die Ausnahme über einen unbegrenzten Jahreszeitraum gelten soll, aktivieren Sie das Optionsfeld **Im Zeitbereich**. Wählen Sie in der Auswahlliste **Startzeit** den Anfang und in der Auswahlliste **Endezeit** das Ende des Tageszeitraums aus.

  Klicken Sie auf **erfolgt täglich**. Wählen Sie im Fenster **Tage auswählen** die Wochentage aus, an denen die Ausnahme gelten soll. Klicken Sie anschließend auf **Speichern**.

- Wenn die Ausnahme über einen begrenzten Jahreszeitraum gelten soll, aktivieren Sie das Optionsfeld **Im Zeit-/Datumsbereich**. Geben Sie im Feld **Startdatum** das Datum für den Beginn und im Feld **Endedatum** das Datum für das Ende des Jahreszeitraums ein (Format tt.mm.jjjj). Wählen Sie in der Auswahlliste **Startzeit** den Anfang und in der Auswahlliste **Endezeit** das Ende des Tageszeitraums aus.

  Klicken Sie auf **erfolgt täglich**. Wählen Sie im Fenster **Tage auswählen** die Wochentage aus, an denen die Ausnahme gelten soll. Klicken Sie anschließend auf **Speichern**.

- Wenn die Ausnahme für die Urlaubszeit gelten soll, aktivieren Sie das Optionsfeld **Urlaubspläne**. Geben Sie im Feld **Startdatum** das Datum für den Beginn und im Feld **Endedatum** das Datum für das Ende der Urlaubszeit ein. Wählen Sie in der Auswahlliste **Startzeit** die Tageszeit für den Anfang und in der Auswahlliste **Endezeit** die Tageszeit für das Ende der Urlaubszeit aus.

  INFO: Urlaubspläne haben Vorrang vor anderen Zeitplänen und Regeln einer Warteschlange.

14) Klicken Sie auf das grüne Speichern-Symbol.

15) Wiederholen Sie die Schritte 10 bis 14, wenn Sie für bestimmte Zeiträume weitere Ausnahmen definieren möchten.

16) Wenn Sie testen möchten, welche Regel (CCV) des Zeitplans an einem bestimmten Zeitpunkt ausgeführt wird, klicken Sie auf **Zeitplan testen**.

Wählen Sie in der Aufklappliste **Datum** den gewünschten Tag und in der Auswahlliste **Zeit** die gewünschte Uhrzeit aus. Klicken Sie auf **Zeitplan testen**. Anschließend wird angezeigt, welche Regel (CCV) an diesem Tag und zu dieser Uhrzeit aktiv ist. Klicken Sie auf **Schließen**, um das Fenster **Zeitplan testen** zu schließen.

17) Wenn Sie diesen Zeitplan einer oder mehreren Warteschlangen zuweisen möchten, klicken Sie auf **Zugewiesene Warteschlangen**. Aktivieren Sie im Fenster **Warteschlangen** die Kontrollkästchen der gewünschen Warteschlange(n). Schließen Sie das Fenster **Warteschlangen**.

18) Schließen Sie das Fenster und bestätigen Sie das Schließen mit **Ja**.

17.6.2.6 Wie Sie einen Zeitplan ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.

4) Klicken Sie auf **Zeitplan**. Alle bereits vorhandenen Zeitpläne werden angezeigt.

5) Markieren Sie den zu ändernden Zeitplan und klicken Sie auf **Bearbeiten**.

6) Ändern Sie die gewünschten Einstellungen für die Standard-CCV:

- Wenn Sie eine andere als die in der Aufklappliste **Standard-CCV** angezeigte Regel (CCV) zuweisen möchten, wählen Sie in der Aufklappliste **Standard-CCV** die gewünschte Regel aus.
- Wenn Sie die in der Aufklappliste **Standard-CCV** angezeigte Regel (CCV) ändern möchten, klicken Sie auf Bearbeiten. Die Regel wird im Regel-Editor angezeigt. Ändern Sie die Regel. Klicken Sie auf **Speichern ...**. Geben Sie den Namen der neuen Regel ein und klicken Sie anschließend auf **OK**. Schließen Sie das Fenster, das das Speichern der Regel bestätigt.

  Wählen Sie in der Aufklappliste **Standard-CCV** die neue, soeben gespeicherte Regel aus.

7) Klicken Sie auf **Zeitplan speichern** und anschließend auf **OK**.

8) Ändern Sie die gewünschten Einstellungen im Fensterbereich **Ausnahmen**:

- Wenn Sie einem bestimmten Zeitraum innerhalb des Zeitplans eine andere Regel (CCV) zuweisen möchten, klicken Sie auf **Hinzufügen**. Wählen Sie in der Aufklappliste dieser Ausnahme die gewünschte Regel aus. Wählen Sie anhand der Optionsfelder und Aufklapplisten, zu welcher

Zeit diese Ausnahme gelten soll. Geben Sie im Feld **Beschreibung** den Namen der Ausnahme ein. Klicken Sie auf das grüne Speichern-Symbol.

- Wenn Sie die oder eine der angezeigten Ausnahmen ändern möchten, klicken Sie auf das Bearbeiten-Symbol der gewünschten Ausnahme. Klicken Sie auf **Bearbeiten**, um die zugehörige Regel (CCV) zu bearbeiten. Die Regel wird im Regel-Editor angezeigt. Ändern Sie die Regel. Klicken Sie auf **Speichern ...**. Geben Sie den Namen der neuen Regel ein und klicken Sie anschließend auf **OK**. Schließen Sie das Fenster, das das Speichern der Regel bestätigt.

  Wählen Sie in der Aufklappliste die neue, soeben gespeicherte Regel aus. Wählen Sie anhand der Optionsfelder und Aufklapplisten, zu welcher Zeit diese Regel (CCV) gelten soll. Klicken Sie auf das grüne Speichern-Symbol.

- Wenn Sie die oder eine der angezeigten Ausnahmen löschen möchten, klicken Sie auf das rote Löschen-Symbol der gewünschten Ausnahme.

9) Wenn Sie testen möchten, welche Regel (CCV) des Zeitplans an einem bestimmten Zeitpunkt ausgeführt wird, klicken Sie auf **Zeitplan testen**. Wählen Sie in der Aufklappliste **Datum** den gewünschten Tag und in der Auswahlliste **Zeit** die gewünschte Uhrzeit aus. Klicken Sie auf **Zeitplan testen**. Anschließend wird angezeigt, welche Regel (CCV) an diesem Tag und zu dieser Uhrzeit aktiv ist. Klicken Sie auf **Schließen**, um das Fenster **Zeitplan testen** zu schließen.

10) Wenn Sie diesem Zeitplan andere Warteschlangen zuweisen möchten, klicken Sie auf **Zugewiesene Warteschlangen**. Aktivieren Sie im Fenster **Warteschlangen** die Kontrollkästchen der Warteschlangen, denen der Zeitplan zugewiesen werden soll. Deaktivieren Sie die Kontrollkästchen der Warteschlangen, denen der Zeitplan nicht zugewiesen werden soll. Schließen Sie das Fenster **Warteschlangen**.

11) Schließen Sie das Fenster und bestätigen Sie das Schließen mit **Ja**.

17.6.2.7 Wie Sie einen Zeitplan löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.

4) Klicken Sie auf **Zeitplan**. Alle vorhandenen Zeitpläne werden angezeigt.

5) Markieren Sie den gewünschten Zeitplan, klicken Sie auf **Entfernen** und anschließend auf **Ja**.

INFO: Ein Zeitplan kann nicht gelöscht werden, solange er einer Warteschlange zugeordnet ist. Vor dem Löschen muss die Zuordnung des Zeitplans zu der oder den Warteschlangen entfernt werden.

17.6.2.8 Wie Sie eine Regel (CCV) als PDF-Datei speichern

Der Wizard **Contact Center** ermöglicht Ihnen das Speichern von Regeln (CCV) als PDF-Datei. Die PDF-Datei kann anschließend beispielsweise ausgedruckt oder per E-Mail verschickt werden.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.

4) Klicken Sie auf **Zeitplan**. Alle bereits vorhandenen Zeitpläne werden angezeigt.

5) Markieren Sie den Zeitplan, der die gewünschte Regel enthält und klicken Sie auf **Bearbeiten**.

6) Wählen Sie in der Aufklappliste die gewünschte Regel aus und klicken Sie auf **Bearbeiten**. Die Regel wird im Regel-Editor angezeigt.

7) Klicken Sie auf **Druckfähiges Bild speichern**. Das Speichern-Fenster erscheint.

8) Geben Sie den Namen der Datei ein und wählen Sie das Verzeichnis aus, in dem die Datei gespeichert werden soll.

9) Klicken Sie auf **Speichern**.

10) Schließen Sie das Fenster und bestätigen Sie das Schließen mit **Ja**.

17.6.2.9 Wie Sie eine Warteschlange hinzufügen

Voraussetzungen

- Mindestens eine UCD-Gruppe wurde eingerichtet.
- Mindestens ein Zeitplan wurde eingerichtet.
- Mindestens ein E-Mail-Account für den E-Mail-Empfang steht zur Verfügung, falls E-Mails in die Warteschlange übernommen werden sollen.
- Der E-Mail-Versand im Kommunikationssystem ist konfiguriert, falls E-Mails durch Agenten der Warteschlange versandt werden sollen.
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.

4) Klicken Sie auf **Warteschlange**.

5) Klicken Sie auf **Hinzufügen**.

6) Klicken Sie auf die Registerkarte **Allgemeine Einstellungen**.

7) Geben Sie im Feld **Name der Warteschlange** den Namen der Warteschlange ein.

Empfehlung: Verwenden Sie den Namen einer der von Ihnen konfigurierten UCD-Gruppen.

INFO: Damit der Name der Warteschlange bei einer Auswertung (Bericht) komplett angezeigt wird, sollten Sie kurze und nicht zusammengesetzte Bezeichnungen wählen. Beispiel: Einkauf Inland Gruppe 1 (nicht: Inlandseinkaufsgruppe 1)

---

8) Wählen Sie eine der folgenden Möglichkeiten für den Zustand der Warteschlange:

- Wenn Sie die neue Warteschlange aktivieren möchten, wählen Sie in der Aufklappliste **Warteschlange aktiv** den Eintrag **Aktiv** aus.
- Wenn Sie die neue Warteschlange deaktivieren möchten, wählen Sie in der Aufklappliste **Warteschlange aktiv** den Eintrag **Nicht aktiv** aus.

  Die Deaktivierung einer Warteschlange führt zur Aktivierung der Rückfalllösung durch die zugehörige UCD-Gruppe. Ist kein Agent bei der UCD-Gruppe angemeldet und kein weiteres Rufweiterschaltungsziel für die UCD-Gruppe eingetragen, wird Anrufern besetzt signalisiert.

9) Geben Sie im Feld **Gruppennummer** die Rufnummer einer UCD-Gruppe ein, die Sie bei der Grundkonfiguration des Contact Centers eingerichtet haben.

10) Wählen Sie in der Aufklappliste **Telefonanlage** den Eintrag **CSP** aus.

11) Wählen Sie in der Aufklappliste **Zeitplan** den gewünschten Zeitplan aus.

12) Geben Sie im Feld **Anzahl Warteschlangen-Alarme** die Alarm-Schwellwertanzahl ein.

Wird die hier angegebene Anzahl wartender Anrufe in der Warteschlange überschritten, wechselt das Warteschlangensymbol bei den Agenten von grün auf orange.

13) Geben Sie im Feld **Zeit Warteschlangen-Alarm** die Alarm-Schwellwertzeit in Sekunden ein.

Wird die hier angegebene Wartezeit eines Anrufs in der Warteschlange überschritten, wechselt der betreffende Eintrag in der Liste der Contact-Center-Anrufe bei den Agenten auf rot.

14) Geben Sie im Feld **Zeitüberschreitung für entgangene Anrufe** die Zeit in Sekunden ein, nach deren Ablauf ein nicht angenommener Anruf zum nächsten freien Agenten weitergeleitet werden soll.

15) Geben Sie im Feld **Schwellwert für abgebrochene Anrufe** die Zeit in Sekunden ein, die festlegt, ob ein abgebrochener Anruf in die Statistik (in einen Bericht) aufgenommen wird oder nicht.

Statistisch erfasst werden Anrufe, die nach Ablauf der angegebenen Zeit abgebrochen werden.

16) Wählen Sie eine der folgenden Möglichkeiten für die Anzeige von PopUp-Fenstern in der Applikation myAgent aus:

INFO: PopUp-Fenster sind erforderlich, um Rückrufe anzunehmen und auszuführen und um Faxe und E-Mails anzunehmen.

- Wenn bei kommenden Anrufen in myAgent ein PopUp-Fenster zur Anzeige und Eingabe von Kundendaten erscheinen soll, aktivieren Sie das Kontrollkästchen **Popup-Fenster aktiviert**.
- Wenn bei kommenden Anrufen in myAgent kein PopUp-Fenster erscheinen soll, deaktivieren Sie das Kontrollkästchen **Popup-Fenster aktiviert**.

17) Wählen Sie eine der folgenden Möglichkeiten für den Nachbearbeitungsmodus:

Bei Warteschlangen mit Nachbearbeitungsmodus können Agenten ihre Anrufe anhand von Nachbearbeitungscodes bestimmten Themen zuordnen (Bestellung, Reklamation, Service usw.).

- Wenn Sie eine Warteschlange mit dem Nachbearbeitungsmodus einfache Nachbearbeitung einrichten möchten, aktivieren Sie die Option **Einfache Nachbearbeitung**.
- Wenn Sie eine Warteschlange mit dem Nachbearbeitungsmodus mehrfache Nachbearbeitung einrichten möchten, aktivieren Sie die Option **Mehrfache Nachbearbeitung**.

- Wenn Sie eine Warteschlange ohne Nachbearbeitungsmodus einrichten möchten, aktivieren Sie die Option **Keine Nachbearbeitung**.

18) Wenn Sie die Priorität der Warteschlange ändern möchten, klicken Sie auf **Prioritäten**.

Klicken und ziehen Sie die roten Punkte im Bereich **Warteschlangen-Priorität im Verlauf der Zeit** auf die gewünschten Positionen. Die horizontale Achse zeigt die Wartezeit in der Warteschlange, die vertikale Achse die Priorität der ausgewählten Warteschlange gegenüber anderen Warteschlangen. Ist ein Agent mehreren Warteschlangen zugeordnet, kann damit festgelegt werden, ob die Anrufe für eine Warteschlange mit höherer Priorität an diesen Agenten weitergeleitet werden sollen als die Anrufe für andere Warteschlangen.

Ziehen Sie die Scrollbalken im Bereich **Anruftyp-Prioritäten** auf die gewünschte Position. Damit legen Sie die Priorität der Anruftypen innerhalb der ausgewählten Warteschlange fest. Je weiter rechts sich der Scrollbalken befindet, desto höher ist die Priorität.

INFO: Für Sprachanrufe sollte eine höhere Priorität als für die anderen Anruftypen gewählt werden. Ansonsten könnten wartende Anrufer durch Rückrufe, Faxe oder E-Mails verdrängt werden.

---

19) Klicken Sie auf die Registerkarte **Warteschlangen-Pilots**.

20) Wenn Faxe in die Warteschlange übernommen werden sollen, aktivieren Sie im Bereich **Pilots für eingehende Faxnachrichten** das oder die Kontrollkästchen des oder der gewünschten Pilots (Rufnummer(n)).

Faxe an diese Rufnummer(n) werden in die Warteschlange übernommen und wie kommende Anrufe behandelt.

21) Wählen Sie eine der folgenden Möglichkeiten im Bereich **Dienst für eingehende E-Mails**, damit E-Mails in die Warteschlange übernommen werden:

- Wenn Sie eine neue E-Mail-Adresse einrichten möchten, klicken Sie auf **Neue E-Mail**. Das Fenster **Warteschlangen-E-Mail-Pilot bearbeiten** wird angezeigt.

  Geben Sie im Feld **Server** die Bezeichnung des E-Mail-Servers ein, der für das Abholen der E-Mails verwendet werden soll (zum Beispiel `pop3.web.de`).

  Geben Sie im Feld **Port** die Portnummer des E-Mail-Servers ein (zum Beispiel `110`, die Standardportnummer für POP3).

  Geben Sie im Feld **Benutzername** und im Feld **Kennwort** die Zugangsdaten für den E-Mail-Server ein.

  Wählen Sie aus, ob der E-Mail-Versand über eine SSL (Secure Socket Layer)-Verbindung erfolgen soll: Wenn Sie eine SSL-Verbindung nutzen möchten, aktivieren Sie das Kontrollkästchen **Verwendet SSL-Verbindung** (Dadurch ändert sich gegebenenfalls die Portnummer des E-Mail-Servers. Standardportnummer für POP3 via SSL = 995). Wenn Sie

keine SSL-Verbindung nutzen möchten, deaktivieren Sie das Kontrollkästchen **Verwendet SSL-Verbindung**.

Klicken Sie auf **OK**. Die neue E-Mail-Adresse wird anschließend im Bereich **Dienst für eingehende E-Mails** angezeigt.

- Wenn Sie eine bestehende E-Mail-Adresse ändern möchten, markieren Sie die gewünschte E-Mail-Adresse und klicken Sie auf **E-Mail bearbeiten**. Das Fenster **Warteschlangen-E-Mail-Pilot bearbeiten** wird angezeigt.

  Ändern Sie die gewünschten Parameter und klicken Sie anschließend auf **OK**.

- Wenn Sie eine bestehende E-Mail-Adresse löschen möchten, markieren Sie die gewünschte E-Mail-Adresse und klicken Sie auf **E-Mail entfernen**.

22) Klicken Sie auf die Registerkarte **Verschiedenes**.

23) Geben Sie im Feld **Absender-E-Mail-Adresse** die E-Mail-Adresse ein, die beim Versenden einer E-Mail durch einen Agenten beim Empfänger angezeigt werden soll.

24) Wählen Sie eine der folgenden Möglichkeiten für die intelligente Anrufweiterleitung innerhalb der Warteschlange aus:

- Wenn kommende Anrufe automatisch an den Agenten weitergeleitet werden sollen, der zuletzt mit dem Anrufer verbunden war, aktivieren Sie das Kontrollkästchen **Nach letztem Agenten des Kunden suchen, wenn kein bevorzugter Agent gefunden wird**. Voraussetzung ist, dass für den Anrufer keine bevorzugten Agenten festgelegt wurden.
- Wenn kommende Anrufe nicht an den Agenten weitergeleitet werden sollen, der zuletzt mit dem Anrufer verbunden war, deaktivieren Sie das Kontrollkästchen **Nach letztem Agenten des Kunden suchen, wenn kein bevorzugter Agent gefunden wird**.

25) Klicken Sie auf **Speichern**.

17.6.2.10 Wie Sie eine Warteschlange ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.

4) Klicken Sie auf **Warteschlange**.

5) Markieren Sie die gewünschte Warteschlange und klicken Sie auf **Bearbeiten**.

6) Klicken Sie auf die Registerkarte **Allgemeine Einstellungen**.

7) Ändern Sie die gewünschten Einstellungen.

8) Wählen Sie eine der folgenden Möglichkeiten für den Zustand der Warteschlange:

- Wenn Sie die Warteschlange aktivieren möchten, wählen Sie in der Aufklappliste **Warteschlange aktiv** den Eintrag **Aktiv** aus.
- Wenn Sie die Warteschlange deaktivieren möchten, wählen Sie in der Aufklappliste **Warteschlange aktiv** den Eintrag **Nicht aktiv** aus.

  Die Deaktivierung einer Warteschlange führt zur Aktivierung der Rückfalllösung durch die zugehörige UCD-Gruppe. Ist kein Agent bei der UCD-Gruppe angemeldet und kein weiteres Rufweiterschaltungsziel für die UCD-Gruppe eingetragen, wird Anrufern besetzt signalisiert.

9) Wählen Sie eine der folgenden Möglichkeiten für die Anzeige von PopUp-Fenstern in der Applikation myAgent aus:

INFO: PopUp-Fenster sind erforderlich, um Rückrufe anzunehmen und auszuführen und um Faxe und E-Mails anzunehmen.

- Wenn bei kommenden Anrufen in myAgent ein PopUp-Fenster zur Anzeige und Eingabe von Kundendaten erscheinen soll, aktivieren Sie das Kontrollkästchen **Popup-Fenster aktiviert**.
- Wenn bei kommenden Anrufen in myAgent kein PopUp-Fenster erscheinen soll, deaktivieren Sie das Kontrollkästchen **Popup-Fenster aktiviert**.

10) Wählen Sie eine der folgenden Möglichkeiten für den Nachbearbeitungsmodus:

Bei Warteschlangen mit Nachbearbeitungsmodus können Agenten ihre Anrufe anhand von Nachbearbeitungscodes bestimmten Themen zuordnen (Bestellung, Reklamation, Service usw.).

- Wenn Sie für die Warteschlange den Nachbearbeitungsmodus einfache Nachbearbeitung einstellen möchten, aktivieren Sie die Option **Einfache Nachbearbeitung**.
- Wenn Sie für die Warteschlange den Nachbearbeitungsmodus mehrfache Nachbearbeitung einstellen möchten, aktivieren Sie die Option **Mehrfache Nachbearbeitung**.
- Wenn Sie für die Warteschlange keinen Nachbearbeitungsmodus einstellen möchten, aktivieren Sie die Option **Keine Nachbearbeitung**.

11) Wenn Sie die Priorität der Warteschlange ändern möchten, klicken Sie auf **Prioritäten**.

Klicken und ziehen Sie die roten Punkte im Bereich **Warteschlangen-Priorität im Verlauf der Zeit** auf die gewünschten Positionen. Die horizontale Achse zeigt die Wartezeit in der Warteschlange, die vertikale Achse die Priorität der ausgewählten Warteschlange gegenüber anderen Warte-

schlangen. Ist ein Agent mehreren Warteschlangen zugeordnet, kann damit festgelegt werden, ob die Anrufe für eine Warteschlange mit höherer Priorität an diesen Agenten weitergeleitet werden sollen als die Anrufe für andere Warteschlangen.

Ziehen Sie die Scrollbalken im Bereich **Anruftyp-Prioritäten** auf die gewünschte Position. Damit legen Sie die Priorität der Anruftypen innerhalb der ausgewählten Warteschlange fest. Je weiter rechts sich der Scrollbalken befindet, desto höher ist die Priorität.

INFO: Für Sprachanrufe sollte eine höhere Priorität als für die anderen Anruftypen gewählt werden. Ansonsten könnten wartende Anrufer durch Rückrufe, Faxe oder E-Mails verdrängt werden.

---

12) Klicken Sie auf die Registerkarte **Warteschlangen-Pilots**.

13) Wählen Sie die gewünschten Einstellungen im Bereich **Pilots für eingehende Faxnachrichten**:

- Wenn Faxe in die Warteschlange übernommen werden sollen, aktivieren Sie im Bereich **Pilots für eingehende Faxnachrichten** das oder die Kontrollkästchen des oder der gewünschten Pilots (Rufnummer(n)).
- Wenn keine Faxe in die Warteschlange übernommen werden sollen, deaktivieren Sie das oder die Kontrollkästchen im Bereich **Pilots für eingehende Faxnachrichten**.

14) Wählen Sie die gewünschten Einstellungen im Bereich **Dienst für eingehende E-Mails**:

- Wenn Sie eine neue E-Mail-Adresse einrichten möchten, klicken Sie auf **Neue E-Mail**. Das Fenster **Warteschlangen-E-Mail-Pilot bearbeiten** wird angezeigt.

  Geben Sie im Feld **Server** die Bezeichnung des E-Mail-Servers ein, der für das Abholen der E-Mails verwendet werden soll (zum Beispiel `pop3.web.de`).

  Geben Sie im Feld **Port** die Portnummer des E-Mail-Servers ein (zum Beispiel `110`, die Standardportnummer für POP3).

  Geben Sie im Feld **Benutzername** und im Feld **Kennwort** die Zugangsdaten für den E-Mail-Server ein.

  Wählen Sie aus, ob der E-Mail-Versand über eine SSL (Secure Socket Layer)-Verbindung erfolgen soll: Wenn Sie eine SSL-Verbindung nutzen möchten, aktivieren Sie das Kontrollkästchen **Verwendet SSL-Verbindung** (Dadurch ändert sich gegebenenfalls die Portnummer des E-Mail-Servers. Standardportnummer für POP3 via SSL = 995). Wenn Sie keine SSL-Verbindung nutzen möchten, deaktivieren Sie das Kontrollkästchen **Verwendet SSL-Verbindung**.

  Klicken Sie auf **OK**. Die neue E-Mail-Adresse wird anschließend im Bereich **Dienst für eingehende E-Mails** angezeigt.

- Wenn Sie eine bestehende E-Mail-Adresse ändern möchten, markieren Sie die gewünschte E-Mail-Adresse und klicken Sie auf **E-Mail**

bearbeiten. Das Fenster **Warteschlangen-E-Mail-Pilot bearbeiten** wird angezeigt.

Ändern Sie die gewünschten Parameter und klicken Sie anschließend auf **OK**.

- Wenn Sie eine bestehende E-Mail-Adresse löschen möchten, markieren Sie die gewünschte E-Mail-Adresse und klicken Sie auf **E-Mail entfernen**.

15) Klicken Sie auf die Registerkarte **Verschiedenes**.

16) Ändern Sie die gewünschten Einstellungen.

17) Klicken Sie auf **Speichern**.

17.6.2.11 Wie Sie eine Warteschlange aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.

4) Klicken Sie auf **Warteschlange**.

5) Klicken Sie auf **Bearbeiten**.

6) Klicken Sie auf die Registerkarte **Allgemeine Einstellungen**.

7) Wählen Sie eine der folgenden Möglichkeiten für den Zustand der Warteschlange:

- Wenn Sie die Warteschlange aktivieren möchten, wählen Sie in der Aufklappliste **Warteschlange aktiv** den Eintrag **Aktiv** aus.
- Wenn Sie die Warteschlange deaktivieren möchten, wählen Sie in der Aufklappliste **Warteschlange aktiv** den Eintrag **Nicht aktiv** aus.

  Die Deaktivierung einer Warteschlange führt zur Aktivierung der Rückfalllösung durch die zugehörige UCD-Gruppe. Ist kein Agent bei der UCD-Gruppe angemeldet und kein weiteres Rufweiterschaltungsziel für die UCD-Gruppe eingetragen, wird Anrufern besetzt signalisiert.

8) Klicken Sie auf **Speichern**.

17.6.2.12 Wie Sie einen Pilot für eingehende Faxnachrichten in Warteschlangen konfigurieren

Voraussetzungen

- Mindestens eine Faxrufnummer für den Empfang von Faxen liegt vor.
- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telephony Server > Teilnehmer**.

3) Klicken Sie im Menübaum auf **Teilnehmer > Applikation-Suite > Contact Center Fax**. Angezeigt werden die für Faxboxen vorgesehenen logischen Portnummern.

4) Klicken Sie im Menübaum auf die gewünschte Portnummer.

5) Klicken Sie auf die Registerkarte **Teilnehmer-Parameter ändern**.

6) Geben Sie im Feld **Rufnummer** die Rufnummer des neuen Pilots für eingehende Faxnachrichten ein.

7) Geben Sie im Feld **Name** den Namen des neuen Pilots für eingehende Faxnachrichten ein.

8) Geben Sie im Feld **Durchwahl** die Durchwahlnummer des neuen Pilots für eingehende Faxnachrichten ein.

9) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Der Pilot für eingehende Faxnachrichten kann jetzt für die gewünschte Warteschlange aktiviert werden.

17.6.2.13 Wie Sie Sollwerte für Servicegrad festlegen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.

4) Klicken Sie auf **Servicegrad**.

5) Markieren Sie die gewünschte Warteschlange und klicken Sie auf **Bearbeiten**.

6) Klicken und ziehen Sie die roten Punkte auf die gewünschten Positionen.

Die horizontale Achse zeigt die Wartezeit in der Warteschlange in Intervallen von 10 Sekunden, die vertikale Achse den Sollwert für den Servicegrad in Prozentwerten.

Damit geben Sie die Sollwerte für die Vermittlungsqualität der Warteschlange vor. Durch den Vergleich der Sollwerte mit den tatsächlichen Anruferwartezeiten können Qualitätsaussagen getroffen werden.

7) Klicken Sie auf **Speichern**.

17.6.2.14 Wie Sie die VIP-Anruferpriorität festlegen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.

4) Klicken Sie auf **VIP-Anruferprioritäten**.

5) Markieren Sie die gewünschte Warteschlange und klicken Sie auf **Bearbeiten**.

6) Klicken und ziehen Sie die roten Punkte auf die gewünschten Positionen.

Damit definieren Sie die Priorität normaler Anrufer gegenüber VIP-Anrufern.

Die horizontale Achse zeigt die Wartezeit in der Warteschlange in Intervallen von 30 Sekunden, die vertikale Achse die Priorität normaler Anrufer, die nicht in der VIP-Rufliste verzeichnet sind.

Beispielsweise können Sie die roten Punkte so festlegen, dass nach 180 Sekunden eine Priorität von 100 Prozent erreicht wird. In diesem Fall werden normale Anrufer erst ab einer Wartezeit von 180 Sekunden gleichberechtigt gegenüber VIP-Anrufern behandelt. Zuvor eingehende Anrufe von VIP-Anrufern werden in der Warteschlange bevorzugt behandelt.

Alternativ können Sie die Werte für die einzelnen Wartezeit-Intervalle auch in die Eingabefelder rechts neben dem Diagramm eingeben.

7) Klicken Sie auf **Speichern**.

17.6.2.15 Wie Sie eine VIP-Rufliste bearbeiten

Voraussetzungen

- Der für die VIP-Rufliste vorgesehene Anrufer steht im externen Verzeichnis.
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.

4) Klicken Sie auf **VIP-Rufliste**.

5) Markieren Sie die gewünschte Warteschlange und klicken Sie auf **Bearbeiten**.

6) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie einen Anrufer in die VIP-Rufliste übernehmen möchten, klicken Sie im oberen Bereich des Fensters auf **Hinzufügen**. Markieren Sie den gewünschten Eintrag. Legen Sie die Priorität dieses VIP-Anrufers gegenüber anderen VIP-Anrufern fest, indem Sie den Scrollbalken auf die gewünschte Position ziehen. Je weiter rechts, desto höher ist die Priorität.
- Wenn Sie ein Rufnummernmuster in die VIP-Rufliste übernehmen möchten, klicken Sie im unteren Bereich des Fensters auf **Hinzufügen**. Geben Sie im Feld Muster das gewünschte Rufnummernmuster ein (zum Beispiel `089 7577*`). Legen Sie die Priorität aller VIP-Anrufer dieses Rufnummernmusters gegenüber anderen VIP-Anrufern fest, indem Sie den Scrollbalken auf die gewünschte Position ziehen. Je weiter rechts, desto höher ist die Priorität.

  Die Eingabe von Rufnummernmustern im kanonischen Rufnummernformat ist nicht möglich. Auch die Verwendung von Abkürzungszeichen für Ländervorwahlen (zum Beispiel +49 statt 0049) ist nicht möglich. Rufnummernmuster sind immer ohne Amtskennziffer anzugeben.

  Beispiel für ein Rufnummernmuster: `089 7577*` (089 = Ortskennzahl München, 7577 = Anlagenrufnummer eines Unternehmens, * = Wildcard für eine beliebige Zahl). Durch den Eintrag dieses Rufnummernmusters in die VIP-Rufliste können alle Anrufer aus München, deren Rufnummer mit 7577 beginnt, bevorzugt behandelt werden.

  Folgende Zeichen können als Wildcards (Platzhalter) in einem Rufnummernmuster verwendet werden:

  * = Wildcard für eine beliebige Zahl

  ? = Wildcard für eine beliebige Ziffer
- Wenn Sie einen Eintrag in der VIP-Rufliste bearbeiten möchten, markieren Sie den gewünschten Eintrag und klicken Sie auf **Bearbeiten**. Ändern Sie die gewünschten Einstellungen.

- Wenn Sie einen Eintrag aus der VIP-Rufliste entfernen möchten, markieren Sie den gewünschten Eintrag und klicken Sie auf **Entfernen**.

7) Klicken Sie auf **Speichern**.

17.6.2.16 Wie Sie einen bevorzugten Agenten festlegen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.

4) Klicken Sie auf **Bevorzugte Agenten**.

5) Markieren Sie die gewünschte Warteschlange und klicken Sie auf **Bearbeiten**.

6) Markieren Sie im Bereich **Kunden** den gewünschten Anrufer.

7) Klicken Sie auf **Agent hinzufügen**.

8) Wählen Sie den gewünschten Agenten aus und klicken Sie auf **OK**.

Anschließend wird der Name des ausgewählten Agenten im Bereich **Bevorzugte Agenten** angezeigt.

9) Wenn Sie einen weiteren Agenten als bevorzugten Agenten festlegen möchten, wiederholen Sie die Schritte 7 und 8.

10) Definieren Sie die Priorität der bevorzugten Agenten, falls mehrere bevorzugte Agenten festgelegt wurden. Sie haben folgende Möglichkeiten:

- Wenn Sie eine höhere Priorität vergeben möchten, markieren Sie den gewünschten Agenten und verschieben Sie diesen über die Schaltfläche **Nach oben** auf eine höhere Listenposition.
- Wenn Sie eine niedrigere Priorität vergeben möchten, markieren Sie den gewünschten Agenten und verschieben Sie diesen über die Schaltfläche **Nach unten** auf eine tiefere Listenposition.

17.6.2.17 Wie Sie einen bevorzugten Agenten löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.
4) Klicken Sie auf **Bevorzugte Agenten**.
5) Markieren Sie die gewünschte Warteschlange und klicken Sie auf **Bearbeiten**.
6) Markieren Sie im Bereich **Bevorzugte Agenten** den oder die zu löschenden Agenten.
7) Klicken Sie auf **Agent entfernen**.

17.6.2.18 Wie Sie eine Contact Center-Pause hinzufügen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.
4) Klicken Sie auf **Contact Center Pausen**.
5) Klicken Sie auf **Hinzufügen**.
6) Geben Sie im Feld **Name** den Namen der neuen Contact Center-Pause ein.
7) Geben Sie im Feld **Dauer (Minuten)** die Dauer der neuen Contact Center-Pause in Minuten ein.
8) Aktivieren Sie das Kontrollkästchen **Aktiv**, um die neue Contact Center-Pause systemweit zu aktivieren.
9) Klicken Sie auf **Speichern**.
10) Wenn Sie eine weitere Contact Center-Pause hinzufügen möchten, wiederholen Sie die Schritte 5 bis 9.

17.6.2.19 Wie Sie eine Contact Center-Pause ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.
4) Klicken Sie auf **Contact Center Pausen**.
5) Markieren Sie die gewünschte Contact Center-Pause und klicken Sie auf **Bearbeiten**.
6) Ändern Sie die gewünschten Parameter.
7) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn die Contact Center-Pause den Agenten zur Verfügung stehen soll, aktivieren Sie das Kontrollkästchen **Aktiv**.
   - Wenn die Contact Center-Pause den Agenten nicht zur Verfügung stehen soll, deaktivieren Sie das Kontrollkästchen **Aktiv**.
8) Klicken Sie auf **Speichern**.

17.6.2.20 Wie Sie eine Contact Center-Pause löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.
4) Klicken Sie auf **Contact Center Pausen**.
5) Markieren Sie die gewünschte Contact Center-Pause und klicken Sie auf **Löschen**.

17.6.2.21 Wie Sie den Nachbearbeitungsgrund für "Einfache Nachbearbeitung" hinzufügen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.

4) Klicken Sie auf **Contact Center Nachbearbeitungs-Codes**. Angezeigt werden alle Warteschlangen für die ein Nachbearbeitungsgrund für "Einfache Nachbearbeitung" definiert wurde.

5) Klicken Sie auf **Hinzufügen**.

6) Wählen Sie in der Aufklappliste **Warteschlange** die Warteschlange aus, für die Sie einen Nachbearbeitungsgrund hinzufügen möchten.

7) Geben Sie im Feld **Beschreibung** eine Bezeichnung für den neuen Nachbearbeitungsgrund ein.

8) Klicken Sie auf **Speichern**.

9) Wenn Sie einen weiteren Nachbearbeitungsgrund hinzufügen möchten, wiederholen Sie die Schritte 5 bis 8.

17.6.2.22 Wie Sie den Nachbearbeitungsgrund für "Einfache Nachbearbeitung" ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.

4) Klicken Sie auf **Contact Center Nachbearbeitungs-Codes**. Angezeigt werden alle Warteschlangen für die ein Nachbearbeitungsgrund für "Einfache Nachbearbeitung" definiert wurde.

5) Markieren Sie den gewünschten Eintrag und klicken Sie auf **Bearbeiten**.

6) Wenn Sie dem Nachbearbeitungsgrund einer anderen Warteschlange zuweisen möchten, wählen Sie in der Aufklappliste **Warteschlange** die neue Warteschlange aus.

7) Wenn Sie die Bezeichnung des Nachbearbeitungsgrunds ändern möchten, geben Sie im Feld **Beschreibung** die neue Bezeichnung ein.

8) Klicken Sie auf **Speichern**.

17.6.2.23 Wie Sie den Nachbearbeitungsgrund für "Einfache Nachbearbeitung" löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.
4) Klicken Sie auf **Contact Center Nachbearbeitungs-Codes**. Angezeigt werden alle Warteschlangen für die ein Nachbearbeitungsgrund für "Einfache Nachbearbeitung" definiert wurde.
5) Markieren Sie den gewünschten Eintrag und klicken Sie auf **Löschen**.

17.6.2.24 Wie Sie den Nachbearbeitungsgrund für "Mehrfache Nachbearbeitung" hinzufügen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.
4) Klicken Sie auf **Mehrfach-Nachbearbeitung Code**.
5) Wählen Sie in der Aufklappliste **Contact Center-Warteschlange** die gewünschte Warteschlange aus. Angezeigt werden die für diese Warteschlange bereits definierten Gruppen und Untergruppen.
6) Wenn Sie den neuen Nachbearbeitungsgrund in einer Gruppe mit weiteren Nachbearbeitungsgründen zusammenfassen möchten, wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie den neuen Nachbearbeitungsgrund einer bestehenden Gruppe oder Untergruppe zuordnen möchten, markieren Sie die gewünschte Gruppe oder Untergruppe und klicken Sie auf **Element hinzufügen**. Geben Sie im Feld **Neues Nachbearbeitungselement** eine Bezeichnung für den neuen Nachbearbeitungsgrund ein und klicken Sie auf **OK**.
   - Wenn Sie den neuen Nachbearbeitungsgrund einer neuen Gruppe zuordnen möchten, klicken Sie auf **Gruppe hinzufügen**. Geben Sie im Feld **Gruppenname** eine Bezeichnung für die neue Gruppe ein und klicken Sie auf **OK**.

     Markieren Sie die neue Gruppe und klicken Sie auf **Element hinzufügen**. Geben Sie im Feld **Neues Nachbearbeitungselement** eine Bezeichnung für den neuen Nachbearbeitungsgrund ein und klicken Sie auf **OK**.
   - Wenn Sie den neuen Nachbearbeitungsgrund einer neuen Untergruppe zuordnen möchten, markieren Sie die gewünschte Gruppe und klicken

Sie auf **Gruppe hinzufügen**. Geben Sie im Feld **Gruppenname** eine Bezeichnung für die neue Untergruppe ein und klicken Sie auf **OK**.

Markieren Sie die neue Untergruppe und klicken Sie auf **Element hinzufügen**. Geben Sie im Feld **Neues Nachbearbeitungselement** eine Bezeichnung für den neuen Nachbearbeitungsgrund ein und klicken Sie auf **OK**.

7) Wenn Sie einen weiteren Nachbearbeitungsgrund hinzufügen möchten, wiederholen Sie die Schritte 5 und 6.

17.6.2.25 Wie Sie den Nachbearbeitungsgrund für "Mehrfache Nachbearbeitung" ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.

4) Klicken Sie auf **Mehrfach-Nachbearbeitung Code**.

5) Wählen Sie in der Aufklappliste **Contact Center-Warteschlange** die gewünschte Warteschlange aus. Angezeigt werden die für diese Warteschlange bereits definierten Gruppen und Untergruppen.

6) Markieren Sie die Gruppe oder Untergruppe, der der zu ändernde Nachbearbeitungsgrund zugeordnet ist. Angezeigt werden alle Nachbearbeitungsgründe (Elemente), die dieser Gruppe zugeordnet sind.

7) Markieren Sie den zu ändernden Nachbearbeitungsgrund und klicken Sie auf **Element umbenennen**.

8) Geben Sie im Feld **Nachbearbeitungscode umbenennen** eine neue Bezeichnung für den Nachbearbeitungsgrund ein und klicken Sie auf **OK**.

9) Wenn Sie die Bezeichnung der Gruppe oder Untergruppe ändern möchten, klicken Sie auf **Gruppe umbenennen**.

10) Geben Sie im Feld **Gruppenname** eine neue Bezeichnung für die Gruppe oder Untergruppe ein und klicken Sie auf **OK**.

17.6.2.26 Wie Sie den Nachbearbeitungsgrund für "Mehrfache Nachbearbeitung" löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.
4) Klicken Sie auf **Mehrfach-Nachbearbeitung Code**.
5) Wählen Sie in der Aufklappliste **Contact Center-Warteschlange** die gewünschte Warteschlange aus. Angezeigt werden die für diese Warteschlange bereits definierten Gruppen und Untergruppen.
6) Markieren Sie die Gruppe oder Untergruppe, der der zu löschende Nachbearbeitungsgrund zugeordnet ist. Angezeigt werden alle Nachbearbeitungsgründe (Elemente), die dieser Gruppe zugeordnet sind.
7) Markieren Sie den zu löschenden Nachbearbeitungsgrund und klicken Sie auf **Element entfernen**.
8) Wenn Sie die Gruppe oder Untergruppe löschen möchten, klicken Sie auf **Gruppe entfernen**.

17.6.2.27 Wie Sie einen Agent einer Warteschlange zuordnen

Mit dem Wizard **Contact Center** können Sie Agenten einer oder mehreren Warteschlangen zuordnen.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.
4) Klicken Sie auf **Warteschlangen-Bindungen**. Alle vorhandenen Warteschlangen und Agenten werden angezeigt.
5) Klicken Sie auf die Warteschlange, der Sie einen Agenten zuordnen möchten. Alle bereits zugeordneten Agenten werden angezeigt.
6) Ziehen Sie den betreffenden Agenten auf die gewünschte Warteschlange. Anschließend wird das Fenster **Agentenzuweisung für Warteschlange** angezeigt.
7) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn der Agent Anrufe unabhängig von der Auslastung der Warteschlange erhalten soll, aktivieren Sie das Optionsfeld **Hauptagent**.
   - Wenn der Agent Anrufe nur bei Überlauf der Warteschlange erhalten soll, aktivieren Sie das Optionsfeld **Agent bei Überlauf**.

8) Wenn Sie **Agent bei Überlauf** gewählt haben:

a) Geben Sie im Feld **Überlauf nach Sekunden in Wartes.** die Zeit ein, nach deren Ablauf ein Anruf an einen Agenten bei Überlauf weitergeleitet werden soll.

b) Geben Sie im Feld **Überlauf nach Anrufen in Wartes.** die Maximalzahl von Anrufen ein. Ein Agent bei Überlauf erhält Anrufe, die über diese Maximalzahl hinausgehen.

9) Stellen Sie einen Prozentwert für das **Fähigkeits-Level** des Agenten ein.

Durch das Fähigkeits-Level steuern Sie die Verteilung der Anrufe auf die Agenten in einer Warteschlange. Agenten mit höherem Fähigkeits-Level werden bei der Anrufverteilung bevorzugt. Haben alle Agenten das gleiche Fähigkeits-Level, erhält der am längsten freie Agent den Anruf.

10) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn der Agent Rückrufwünsche in Form von Sprachnachrichten erhalten soll, aktivieren Sie das Kontrollkästchen **Agentenrückruf aktivieren**.
- Wenn der Agent keine Rückrufwünsche erhalten soll, deaktivieren Sie das Kontrollkästchen **Agentenrückruf aktivieren**.

11) Geben Sie im Feld **Nachbearbeitung** die automatische Nachbearbeitungszeit in Sekunden für den Agenten in dieser Warteschlange ein.

12) Klicken Sie auf **OK**.

13) Wenn Sie weitere Agenten den Warteschlangen zuordnen möchten, wiederholen Sie die Schritte 5 bis 12.

17.6.2.28 Wie Sie einen Agent aus einer Warteschlange entfernen

Mit dem Wizard **Contact Center** können Sie Agenten aus einer oder mehreren Warteschlangen entfernen.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Contact Center** zu starten.

4) Klicken Sie auf **Warteschlangen-Bindungen**. Alle vorhandenen Warteschlangen und Agenten werden angezeigt.

5) Doppelklicken Sie auf die Warteschlange, aus der Sie einen Agenten entfernen möchten. Alle zugeordneten Agenten werden angezeigt.

6) Klicken Sie mit der rechten Maustaste auf den gewünschten Agenten und wählen Sie im Aufklappmenü **Entfernen**.

7) Wenn Sie weitere Agenten aus Warteschlangen entfernen möchten, wiederholen Sie die Schritte 5 und 6.

17.7 Hinweise zum Einsatz des Contact Centers

Hier erhalten Sie Informationen über Besonderheiten und mögliche Einschränkungen beim Einsatz des Contact Centers.

17.7.1 Einschränkungen beim Betrieb des Contact Centers

Für den Betrieb des Contact Centers gelten bestimmte Bedingungen. Darüber hinaus kommt es zu Einschränkungen bei der Nutzung von System-Leistungsmerkmalen durch Agenten.

Bedingungen für den Betrieb des Contact Centers

Folgende Bedingungen für den Betrieb des Contact Centers sind zu beachten:

- Leitungen
  Das Contact Center unterstützt keine analogen Amtsleitungen (HKZ). Alle externen Verbindungen des Contact Centers müssen über ISDN oder über IP-Telefonie erfolgen. Zu beachten ist, dass die Anbindung über IP-Telefonie ausschließlich über zertifizierte Internet-Telefonie-Service-Provider ITSP möglich ist.
- Vernetzung
  Bei einer Vernetzung müssen alle Agenten an dem Kommunikationssystem angeschlossen sein, in dem das Contact Center konfiguriert ist.
- Agententelefone
  Agenten können alle Systemtelefone (IP-Telefone (HFA), wie zum Beispiel OpenStage 40 oder $U_{P0/E}$-Telefone, wie zum Beispiel OpenStage 40 T) und DECT-Telefone nutzen. Zu beachten ist, dass ausschließlich die aktuell für den Betrieb mit OpenScape Business Cordless freigegeben DECT-Telefone eingesetzt werden dürfen.
  Die Verwendung von analogen, ISDN- und SIP-Telefonen ist nicht möglich.
  Agenten dürfen nicht Mitglied einer Gruppe (Gruppenruf, Sammelanschluss) oder eine MULAP sein. Diese Einschränkung gilt auch für die in Verbindung mit MULAPs genutzten System-Leistungsmerkmale "Teamschaltung (Team-Gruppe)", "Chef/Sekretär (Top-Gruppe)" und "Mobility Entry".
- myAgent
  myAgent sollte nicht simultan mit anderen UC-Clients genutzt werden, da eine gegenseitige Beeinflussung des Anwesenheitsstatus nicht ausgeschlossen ist (siehe *Hinweise zur gleichzeitigen Nutzung von myAgent und UC Suite Clients*). Im Normalbetrieb des Contact Centers verwenden Agenten ausschließlich myAgent, um ihren Status zu ändern (Anmelden, Abmelden, Verfügbar usw.).

- Anschaltung von Applikationen über die CSTA-Schnittstelle
  Sofern die folgende Bedingungen eingehalten werden, ist eine Anschaltung von Applikationen über die CSTA-Schnittstelle möglich:
  - Die Applikation darf keine nennenswerte Zusatzlast auf der CSTA-Schnittstelle erzeugen.
    Dementsprechend ist die Anschaltung von Unified-Communications- oder Anrufverteil-Lösungen, CTI-Power-Dialern oder auch CTI-Lösungen mit vielen intensiv genutzten CTI-Einzel-Clients nicht zugelassen.
  - Die Applikation darf über die CSTA-Schnittstelle keine Agententelefone steuern oder Umleitungen für die Agententelefone einrichten.
    Dementsprechend ist die Anschaltung von CTI-Applikationen für Agenten, Regelassistenten oder Personal Assistants nicht zugelassen.

  Die Anschaltung von TAPI 120/170 ist prinzipiell freigegeben. Für die Belastung des Kommunikationssystems gelten die gleichen Bedingungen, wie für die Anschaltung anderer Applikationen über die CSTA-Schnittstelle. In Verbindung mit dem Contact Center sollte TAPI 120/170 vorzugsweise zur Anbindung von CRM (Customer Relationship Management)-/ERP (Enterprise Ressource Planning)-Systemen verwendet werden, sofern diese TAPI unterstützen.

Einschränkungen bei der Nutzung von System-Leistungsmerkmalen

Die nachfolgend genannten System-Leistungsmerkmale stehen für Agenten nicht oder nur mit Einschränkungen zur Verfügung. Diese Leistungsmerkmale sind aber für Agenten nicht zwingend notwendig, da die Zuteilung von Anrufen automatisch durch das Contact Center erfolgt. Die Zuteilung ist abhängig von den eingestellten Regeln und der Verfügbarkeit der Agenten.

- Gesperrte Leistungsmerkmale
  Die Aktivierung von System-Leistungsmerkmalen über myAgent und über das zugehörige Agententelefon wird für verfügbare Agenten des Contact Centers nicht unterstützt. Agenten können System-Leistungsmerkmale ausschließlich über myAgent aktivieren.
  Die folgenden System-Leistungsmerkmale werden deshalb in Verbindung mit myAgent nicht unterstützt:
  - Anklopfen
  - Zweitanruf
  - Parken
  - Gruppenruf
  - Anrufschutz (für angemeldete Agenten)
  - Aufschalten auf ein Agentengespräch (Ausnahme: Agenten mit dem Berechtigungs-Level Supervisor oder Administrator)
  - Leistungsmerkmale, die das Anruf-Routing betreffen und aktive Gesprächsverbindungen
- Leistungsmerkmale mit Auswirkungen auf das Anruf-Routing
  Folgende Leistungsmerkmale können zu einer Veränderung des Anruf-Routings im Contact Center führen und sollten deshalb von Agenten nicht ausgeführt werden.

  - Anrufumleitung
    Aktiviert ein angemeldeter Agent eine Anrufumleitung, erfolgt eine Abmeldung.
    Eine Anrufumleitung wird deaktiviert, sobald sich ein Agent an einer Warteschlange anmeldet.
  - Anrufschutz
    Aktiviert ein angemeldeter Agent den Anrufschutz über einen UC-Client, erfolgt eine Abmeldung.
    Anrufschutz wird deaktiviert, sobald sich ein Agent an einer Warteschlange anmeldet.
  - Relocate
    Durch das Umziehen eines Telefons wird die logische Zuordnung der Rufnummern verändert. Die neue Rufnummernzuordnung wird erst nach einem Restart (Neustart) des Contact Centers übermittelt.
  - Nachtschaltung
    Bei der Einrichtung einer Nachtschaltung im Kommunikationssystem ist darauf zu achten, dass die Konfiguration der Contact-Center-relevanten Parameter (Agenten, Warteschlangen usw.) für den Tag- und Nachtbetrieb identisch ist.
- Leistungsmerkmale mit Auswirkungen auf Berichte
  Die Ausführung folgender Leistungsmerkmale von einem Agenten-Telefon kann zu einer Verfälschung von Berichten führen.
  - Anrufübernahme von Contact-Center-Anrufen durch Nicht-Agenten
  - Anrufübergabe (zum Beispiel über Direktruftaste) von Contact-Center-Anrufen an Nicht-Agenten
  - Konferenz
  - Makeln
  - Parken

  INFO: Das Leistungsmerkmal "Rückfrage" ist für die Darstellung von Contact-Center-Anrufen in Berichten neutral und kann durch Agenten genutzt werden, unabhängig vom Rückfrageziel.

- Für Agenten nicht sinnvolle Funktionen
  Folgende Funktionen sind nicht sinnvoll, da für Agenten das Leistungsmerkmal "Anklopfen" gesperrt ist.
  - Vermittlungsplatz
  - Hotline-Ziel

17.8 Hinweise zum Einsatz von DECT-Telefonen

DECT-Telefone können als Telefone für Contact-Center-Agenten eingesetzt werden. Unterschiede bei der Bedienprozedur gegenüber schnurgebundenen Telefonen sind dabei zu beachten.

Voraussetzungen für den Einsatz von DECT-Telefonen

- Ausschließlich die aktuell für den Betrieb mit HiPath Cordless Office und OpenScape Business Cordless freigegeben DECT-Telefone dürfen verwendet werden.
- Der Bereich, in dem sich die Contact-Center-Agenten bewegen, muss eine lückenlose Funkabdeckung bieten.
- Die Anzahl der Basisstation muss so bemessen sein, dass genügend B-Kanäle für die DECT-Telefone der Contact-Center-Agenten zur Verfügung stehen.
- Ein Contact-Center-Agent sollte den Funkbereich möglichst nicht verlassen, während er an einer Warteschlange des Contact Centers angemeldet ist.

Unterschiede bei der Bedienprozedur gegenüber schnurgebundenen Telefonen

- Das Anmelden an einer Warteschlange des Contact Centers ist ausschließlich über myAgent möglich.
- Im Display eines DECT-Telefons werden keine Meldungen angezeigt, wie zum Beispiel **Verfügbar** oder **Pause**.
- Die Steuerung eines DECT-Telefons über myAgent (zum Beispiel über den Bereich **Telefonie** des myAgent-Hauptfensters oder über das PopUp-Fenster des ankommenden myAgent-Anrufs) ist nicht möglich.
- Die Annahme eines ankommenden Anrufs ist ausschließlich über das DECT-Telefon möglich.
- Ein gehender Anruf muss über das DECT-Telefon initiiert werden.

Zu berücksichtigende Effekte beim Einsatz von DECT-Telefonen:

- Suchzeit
  Bei einem ankommenden Anruf kann die Zeit bis zum Finden des DECT-Telefons mehrere Sekunden (im ungünstigsten Fall bis zu 20 Sekunden) betragen, bevor ein Anruf am DECT-Telefon signalisiert wird. Während der Suchzeit hört der Anrufer den Rufton.
  Das Contact Center wertet diese Zeit als Zeit bis zur Anrufannahme. Die eigentliche Zeit bis zur Anrufannahme durch einen Contact-Center-Agenten setzt sich damit aus der Suchzeit und der Klingeldauer zusammen.
  Verlässt ein Contact-Center-Agent mit seinem DECT-Telefon den Funkbereich, können sich längere Suchzeiten ergeben.
- DECT-Telefon nicht auffindbar
  Überschreitet ein Contact-Center-Anruf die vorgegebene Zeit bist zur Rufannahme durch den Agenten (Contact-Center-Agent befindet sich beispielsweise außerhalb des Funkbereichs), wird der Agent automatisch von der oder den Warteschlangen abgemeldet. Das Wiederanmelden ist ausschließlich über myAgent möglich.

17.9 Berichte

Anhand von Berichten kann der aktuelle Status des Contact Centers ermittelt und die Stärken und Schwächen der zugehörigen Komponenten analysiert werden.

Das ermöglicht beispielsweise eine Optimierung der Contact-Center-Konfiguration und einen effizienteren Einsatz der Contact-Center-Ressourcen. Das Contact Center stellt Anwendern sowohl Echtzeit-Berichte als auch historische Berichte zur Verfügung.

Echtzeit-Berichte

Echtzeit-Berichte werden ständig aktualisiert. Sie liefern wichtige Informationen, wie zum Beispiel Angaben zur Agenten-Auslastung, zum Servicegrad, zu Abbruchraten und zu durchschnittlicher Bearbeitungszeiten. Anhand der fortwährend aktualisierten und filterbaren Anruferlisten kann der Verlauf eines Kundenkontakts schrittweise untersucht werden. Darüber hinaus ist die Prüfung der Aktivitäten aller Agenten möglich. Diese Informationen können beispielsweise für Schulungszwecke, Kontaktprüfungs- und Nachverfolgungsaktivitäten eingesetzt werden.

Agenten mit dem Berechtigungs-Level Supervisor oder Administrator können akustisch und visuell darüber informiert werden, wenn definierbare Betriebsmessgrößen überschritten werden. Die Festlegung der entsprechenden Schwellwerte ist für jede Warteschlange individuell möglich.

Historische Berichte

Durch die Auswahl von Datenelementen und benutzerspezifischen Berichtsparametern können historische Berichte schnell eingerichtet und in Grafik- oder Tabellenform abgerufen werden.

Über die Applikation myAgent können mehr als 20 vordefinierte Berichtsvorlagen für Standardberichte genutzt werden.

Der optional einsatzbare Applikation myReports erweitert die Möglichkeiten zur Erstellung historischer Berichte durch über 100 vordefinierte Berichtsvorlagen. Die Berichtserstellung kann individuell geplant und die erstellten Berichte können zu festgelegten Zeiten in gängigen Exportformaten automatisch an zuvor festgelegte E-Mail-Empfänger versendet oder an einem vom myReports-Administrator konfigurierten Speicherort abgelegt werden. Versierte und mit den Datenbankstrukturen vertraute Anwender haben über den in myReports integrierten BIRT (Business Intelligence and Reporting Tools) RCP Designer die Möglichkeit, vordefinierte Berichtsvorlagen zu verändern oder neue Berichtsvorlagen zu erstellen.

INFO: Berichte basieren auf der im Kommunikationssystem gespeicherten Anrufhistorie. Die maximale Aufbewahrungsdauer der Anrufhistorie beträgt 365 Tage (Standardeinstellung). Ein Administrator mit dem Profil **Expert** kann die Aufbewahrungsdauer der Anrufhistorie systemweit einstellen.

Beispiel: Die Aufbewahrungsdauer wurde auf 100 Tage eingestellt. Für die Erstellung von Berichten kann damit auf Daten zurückgegriffen werden, die maximal 100 Tage alt sind.

Datenschutz

Hat der myReports-Administrator bei der Konfiguration von myReports den Datenschutz aktiviert, werden in allen betreffenden Berichten die letzten vier Stellen der Rufnummern (Spalte CLI) durch **** ersetzt.

Hat ein interner Teilnehmer seine private Rufnummer, Mobilrufnummer, externe Rufnummer 1 und/oder externe Rufnummer 2 als nicht sichtbar gekennzeichnet, werden diese Rufnummern in allen betreffenden Berichten nicht angezeigt.

17.9.1 Vordefinierte Berichtsvorlagen

myReports stellt mehr als 100 vordefinierte Berichtsvorlagen zur Verfügung, um Berichte zu erstellen.

Diese Vorlagen sind folgenden Themengebieten (Berichtgruppen) zugeordnet:

- **Agententätigkeit**
- **Agenten**
- **CLI**
- **Anrufhistorie**
- **Anrufe**
- **Fax / E-Mail**
- **Andere**
- **Leistung**
- **Warteschlangen**
- **Benutzer-Anwesenheitsstatus**
- **Nachbearbeitungscodes**

17.9.2 Berichts-Designer

Der in myReports integrierte Berichts-Designer ermöglicht die Definition eigener Berichtsvorlagen.

Der Berichts-Designer ist eine separat startende Open-Source-Anwendung (BIRT (Business Intelligence and Reporting Tools) RCP Designer) für die professionelle Erstellung von Berichtsvorlagen.

myReports unterstützt den BIRT RCP Designer durch

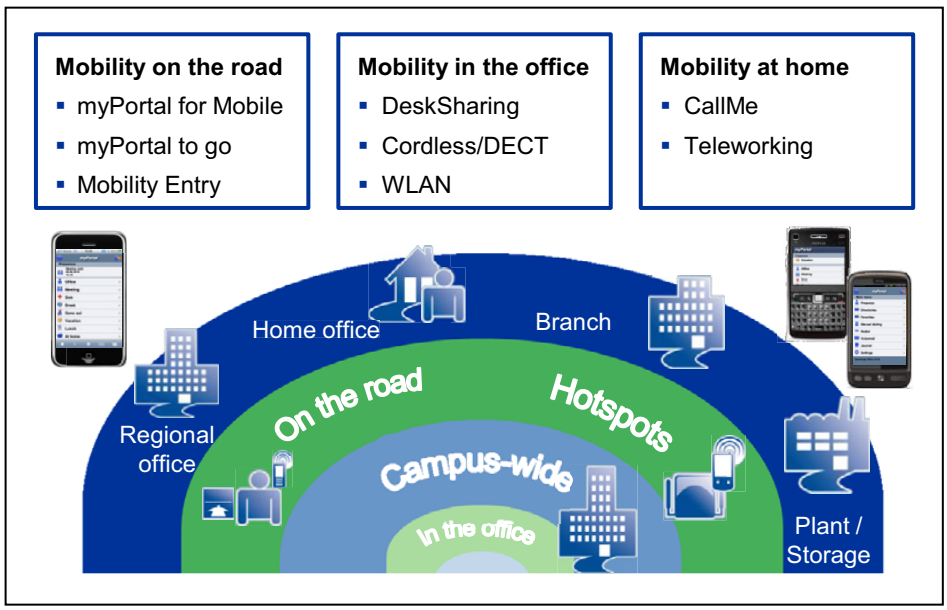
- die Vordefinition der Datenbankanbindung.
- die Einbindung der in myReports verwendeten Berichtsvorlagen.
- ein Datentransferprogramm zur Integration der neu erstellten Berichtsvorlagen in den Report Manager.

18 Mobility

OpenScape Business bietet integrierte Mobilitätslösungen für jedes Unternehmen. Dies beinhaltet z. B. die Einbindung von Mobiltelefonen/Smartphones, die Nutzung von Cordless/DECT- und WLAN-Telefonen bis hin zu DeskSharing und Teleworking. Mobility umfasst Mobilität unterwegs, Mobilität im Büro und Mobilität zu Hause.

18.1 Integrierte Mobilitätslösungen

Die im Kommunikationssystem integrierten Mobilitätslösungen bieten effiziente Kommunikation überall und mit unterschiedlichsten Endgeräten.



18.2 Mobilität unterwegs

Mobilität unterwegs wird erreicht über die Mobiltelefon-Integration über myPortal for Mobile, myPortal to go oder Mobility Entry. Über den One Number Service ist der Teilnehmer weltweit unter einer Rufnummer erreichbar. Über Dual-Mode-Telefonie können zusätzlich Kosten gespart werden, wenn sich der Teilnehmer in Reichweite eines WLAN befindet.

Mobilität unterwegs ist die Kombination von:

- Bürotelefon und Smartphone (myPortal for Mobile, myPortal to go)
  - Erreichbarkeit unter einer Rufnummer (One Number Service)
  - Steuerung von Leistungsmerkmalen über Web-Client
  - UC-Funktionen wie z. B. Steuerung des Anwesenheitsstatus

- Bürotelefon und Mobiltelefon (Mobility Entry)
  - Erreichbarkeit unter einer Rufnummer (One Number Service
  - Steuerung von Leistungsmerkmalen über DTMF-Codes

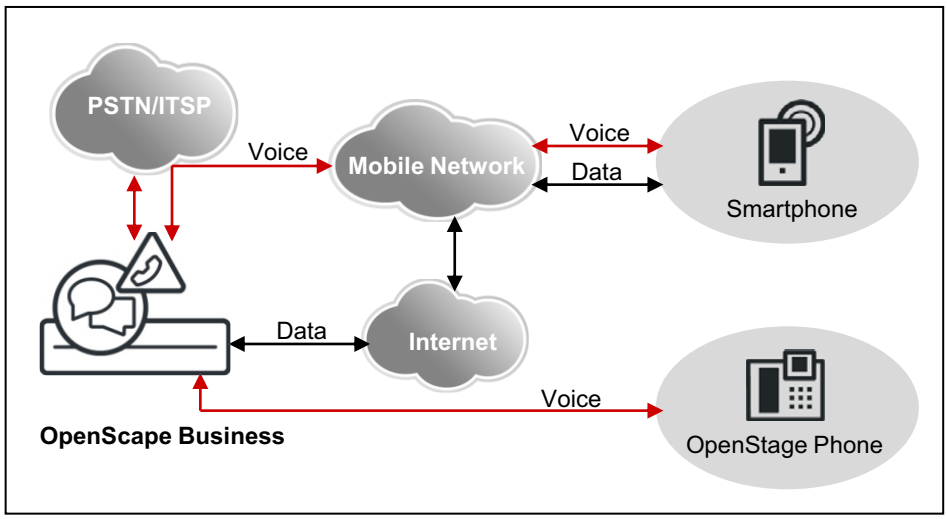
Neben der Kombination von Mobiltelefon und Bürotelefon ist es auch möglich, ein Mobiltelefon alleine (d. h. ohne paralleles Bürotelefon) für die Erreichbarkeit unter einer Festnetznummer zu konfigurieren.

Der volle Funktionsumfang wird mit Systemtelefonen (HFA) erreicht. SIP-Telefone können mit Einschränkungen verwendet werden.

18.2.1 myPortal for Mobile

myPortal for Mobile integriert Mobiltelefone in das Kommunikationssystem. Dadurch hat der Teilnehmer über den Web-Browser des Mobiltelefons Zugriff auf Unified-Communications-Leistungsmerkmale analog zu myPortal for Desktop oder myPortal for Outlook.

Bei myPortal for Mobile steuert das Mobiltelefon das Kommunikationssystem über Web-Browser. myPortal for Mobile baut eine parallele Datenverbindung zum Kommunikationssystem auf und bietet dadurch zusätzlich Unified Communications wie z. B. Anwesenheitsstatus, Verzeichnisse und Journale. myPortal for Mobile kann sowohl auf reinen GSM-Mobiltelefonen als auch auf Dual-Mode-Telefonen genutzt werden. Für die Nutzung von myPortal for Mobile ist ein Mobilfunkvertrag mit Datenoption (Flatrate empfohlen) erforderlich.



Leistungsmerkmale für myPortal for Mobile

- Verzeichnisse
- Favoritenliste
- Journal
- Anwesenheitsstatus
- CallMe-Dienst (nur UC Suite)
- Sprachnachrichten

CTI-Leistungsmerkmale während eines Gesprächs

- Rückfrage
- Makeln
- Vermitteln
- Konferenz
- Trennen

Aufruf von myPortal for Mobile

Der mobile Teilnehmer kann über den Web-Browser seines Mobiltelefons auf myPortal for Mobile zugreifen. Die URLs sind:

`http://<IP-Adresse des Kommunikationssystems>:8801`

`https://<IP-Adresse des Kommunikationssystems>:8802`

Aus Sicherheitsgründen wird empfohlen ausschließlich https zu verwenden. Dafür muss im Router ein Port Forwarding von extern TCP/443 nach intern TCP/8802 eingerichtet werden.

Nach erfolgreicher Verbindung mit dem Kommunikationssystem wird im Web-Browser der Anmelden-Bildschirm mit Benutzername (= interne Rufnummer des Teilnehmers) und das Passwort (= Passwort für myPortal) angezeigt.

Wahlverfahren von myPortal for Mobile

Für gehende Gespräche kann der Mobiltelefon-Teilnehmer zwischen unterschiedlichen Wahlverfahren wählen:

- Callback
- Call Through
- SIP
- Assoziierte Wahl (nur für Tablet-PC)
  Wird über die assoziierte Wahl ein SIP-Telefon oder ein SIP-Softclient gesteuert, stehen einige CTI-Leistungsmerkmale wie Rückfrage und Konferenz nicht zur Verfügung.

Verwandte Themen

- One Number Service
- Vergleich Mobile Clients und Mobility Entry
- Abhängigkeiten für Mobile Clients und Mobility Entry

18.2.1.1 Voraussetzungen für myPortal for Mobile

Um myPortal for Mobile zu nutzen muss das Mobiltelefon oder der Tablet-PC über geeignete Hardware und Software verfügen.

Es gelten folgende Anforderungen:

Client	Technische Daten
myPortal for Mobile	myPortal for Mobile ist optimiert für die Darstellung auf Apple iPhone und mit zahlreichen anderen Mobiltelefonen funktionsfähig. Abhängig vom verwendeten Gerät und Betriebssystem können Bedienkomfort oder Funktion beeinflusst werden. Es gelten folgende Anforderungen: • Touchscreen (empfohlen für komfortable Bedienung) • Display-Auflösung mindestens 240 Pixel * 320 Pixel • Internetzugang • Webbrowser mit aktiviertem JavaScript • Unterstützung der gleichzeitigen Übertragung von Sprache und Daten durch Mobiltelefon und Mobilnetz • 3G-Datenverbindung, z. B. EDGE, UMTS, HSDPA (empfohlen für flüssige Bedienung). GPRS kann zu langsamem Seitenaufbau führen. • Datenflatrate (empfohlen aus Kostengründen), da je nach Nutzungsverhalten Datenvolumina von mehreren 100 Mbyte pro Monat anfallen können.
myPortal for Mobile (for Tablet-PC)	myPortal for Mobile/Tablet-PC ist optimiert für die Darstellung auf Apple iPad und mit zahlreichen anderen Tablet-PC funktionsfähig. Abhängig vom verwendeten Gerät und Betriebssystem können Bedienkomfort oder Funktion beeinflusst werden. Es gelten folgende Anforderungen: • Touchscreen (empfohlen für komfortable Bedienung) • Display-Auflösung mindestens 800 Pixel * 480 Pixel empfohlen mindestens 1024 Pixel * 600 Pixel • Internetzugang • Webbrowser mit aktiviertem JavaScript • 3G-Datenverbindung, z. B. EDGE, UMTS, HSDPA (empfohlen für flüssige Bedienung). GPRS kann zu langsamem Seitenaufbau führen. Alternativ: reine WLAN-Verbindung mit einem SIP-Client für Telefonie. • Datenflatrate (empfohlen aus Kostengründen), da je nach Nutzungsverhalten Datenvolumina von mehreren 100 Mbyte pro Monat anfallen können.

Abhängig vom verwendeten Gerät und Betriebssystem können Bedienkomfort oder Funktion beeinflusst werden. Support wird nur geleistet, wenn ein Problem mit einem Referenzgerät nachweisbar ist. Informationen zu den Referenzgeräten, Browsern und Betriebssystemen finden Sie in der Freigabbemitteilung und im Experten-Wiki: `http://wiki.unify.com/wiki/myPortal_for_Mobile`.

18.2.2 myPortal to go

myPortal to go ist eine leistungsfähige Unified Communications Anwendung für Smartphones und Tablet-PCs und bietet den Teilnehmern Zugriff auf die Unified

Communications Leistungsmerkmale des Kommunikationssystems. Neben komfortablen Wahlhilfen über Verzeichnisse und Favoriten sowie Informationen über den Anwesenheitsstatus von Kollegen wird auch der Zugriff z. B. auf Sprachnachrichten zur Verfügung gestellt.

myPortal to go gibt es in drei Varianten:

- als Mobile UC App für das Betriebssystem Android (Version 4.0 oder höher)
- als Mobile UC App für das Betriebssystem Apple iOS (Version 6 oder höher)
- als Web Edition für mobile Web-Browser mit HTML5-Unterstützung, z. B. für Betriebssysteme Windows Phone (Version 8.0 oder höher) oder Blackberry (Version 10 oder höher)

Der Leistungsumfang ist für die Varianten bis auf wenige Ausnahmen (z. B. Zugriff auf Kontaktdaten im Mobiltelefon) identisch.

myPortal to go unterstützt folgende Leistungsmerkmale:

- Anwesenheitsstatus
- Statusbezogene Anrufumleitung
- CallMe-Dienst (nur mit UC Suite)
- Verzeichnisse
- Favoritenliste
- Journal
- Rufnummern- und Namenssuche
- Anruffunktionen
- One Number Service
- Sprachnachrichten
- Textnachrichten

myPortal to go kann mit beiden UC-Lösungen UC Smart und UC Suite verwendet werden. Je nach UC-Lösung und den Ihnen zugeordneten Lizenzen kann das Angebot der Leistungsmerkmale leicht variieren.

myPortal to go unterstützt folgende Betriebsarten:

- Mobiler Benutzer:
  Uneingeschränkter Zugriff auf die Telefonie- und UC-Leistungsmerkmale unabhängig von Standort (inkl. One Number Service).
- Office-Benutzer:
  Nutzung der UC-Leistungsmerkmale und als Komfort-Wahlhilfe für das Bürotelefon (ohne One Number Service).

Weitere Leistungsmerkmale können Sie mit den UC Clients (z. B. myPortal Smart oder myPortal for Desktop) nutzen.

myPortal to go stellt eine verschlüsselte Verbindung (https) zum OpenScape Business UC Server her. Ist die Verbindung unterbrochen (Offline-Modus) können Sie noch zwischengespeicherte Einträge aus dem Journal und der Favoritenliste per GSM wählen sowie eine manuelle GSM-Wahl ausführen.

Wahlverfahren von myPortal to go

Für gehende Gespräche kann der Smartphone-Teilnehmer abhängig von der Betriebsart zwischen unterschiedlichen Wahlverfahren wählen:

- Call through (nur in der Betriebsart Mobiler Benutzer)
- Callback bevorzugt (nur in der Betriebsart Mobiler Benutzer)
- Assoziierte Wahl (nur in der Betriebsart Office-Benutzer)
  myPortal to go steuert den Verbindungsaufbau für das Telefon am Arbeitsplatz. Wird über die assoziierte Wahl ein SIP-Telefon oder ein SIP-Softclient gesteuert, stehen einige CTI-Leistungsmerkmale wie Rückfrage und Konferenz nicht zur Verfügung.

18.2.2.1 Voraussetzungen für myPortal to go

Um myPortal to go zu nutzen muss das Smartphone oder der Tablet-PC über geeignete Hardware und Software verfügen.

Es gelten folgende Anforderungen:

- Für myPortal to go als Mobile UC App: Betriebssystem Android (Version 4.0 oder höher) oder Apple iOS (Version 6 oder höher)
- Für myPortal to go als Web Edition: mobile Web-Browser mit HTML5-Unterstützung, z. B. für Betriebssysteme Windows Phone (Version 8.0 oder höher) oder Blackberry (Version 10 oder höher)
  Für den Zugriff muss im Router ein Port Forwarding von extern TCP/443 nach intern TCP/8802 (https) oder TCP/8801 (http) eingerichtet werden. Aus Sicherheitsgründen wird empfohlen ausschließlich https zu verwenden.
- Touchscreen (empfohlen für komfortable Bedienung)
- Display-Auflösung mindestens 240 Pixel * 320 Pixel (empfohlen: 320 Pixel * 480 Pixel oder höher)
- Internetzugang
- Unterstützung der gleichzeitigen Übertragung von Sprache und Daten durch Mobiltelefon und Mobilnetz
- 3G-Datenverbindung, z. B. EDGE, UMTS, HSDPA (empfohlen für flüssige Bedienung). GPRS kann zu langsamem Seitenaufbau führen.
- Datenflatrate (empfohlen aus Kostengründen), da je nach Nutzungsverhalten Datenvolumina von mehreren 100 Mbyte pro Monat anfallen können.

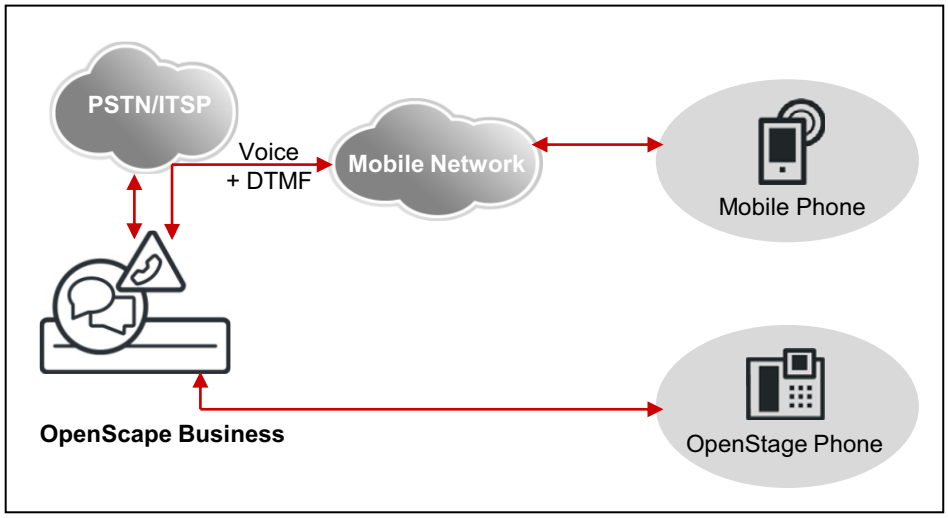
Die Mobile UC App kann kostenfrei im Google Play Store oder im Apple App Store heruntergeladen werden.

Abhängig vom verwendeten Gerät und Betriebssystem können Bedienkomfort oder Funktion beeinflusst werden. Support wird nur geleistet, wenn ein Problem mit einem Referenzgerät nachweisbar ist. Informationen zu den Referenzgeräten, Browsern und Betriebssystemen finden Sie in der Freigabbemitteilung und im Experten-Wiki: `http://wiki.unify.com/wiki/myPortal_to_go`.

18.2.3 Mobility Entry

Durch Mobility Entry können Mobiltelefone integriert werden. Dadurch hat der Teilnehmer über das Mobiltelefon Zugriff auf bestimmte System-Leistungsmerkmale.

Mobility Entry ermöglicht nach Einwahl die Steuerung von Sprachverbindungen über DTMF.



Wahlverfahren von Mobility Entry

Für gehende Gespräche kann der Mobiltelefon-Teilnehmer zwischen unterschiedlichen Wahlverfahren wählen.

Mobility Entry bietet folgende Wahlverfahren:

- Callback
- Call Through

Ruft bei Callback der Mobiltelefon-Teilnehmer am Kommunikationssystem eine spezielle Durchwahlnummer an, dann wird der Anruf noch vor dem Aufbau der Verbindung automatisch getrennt und es wird sofort ein Rückruf (Callback) durchgeführt. Nach dem Rückruf ist keine weitere Autorisierung notwendig. Der Mobiltelefon-Teilnehmer kann über das Kommunikationssystem interne und externe Anrufe durchführen sowie alle Mobility-Leistungsmerkmale nutzen.

Voraussetzungen für Callback sind:

- Die externe Rufnummer des anrufenden Telefons ist am Kommunikationssystem registriert und konfiguriert. Wenn nicht, wird der Anruf getrennt und kein Rückruf durchgeführt.
- Die DISA-Durchwahlnummer ist konfiguriert.
- Die externe Rufnummer des Mobiltelefon-Teilnehmers wird zum Kommunikationssystem übertragen (CLIP-Information).

Leistungsmerkmale im Ruhezustand

- Rufnummer wählen

- Anrufumleitung programmieren oder löschen
- Anrufschutz aktivieren oder deaktivieren
- Info senden
- Alle Dienste zurücksetzen
- Rufnummernunterdrückung (CLIR) ein- oder ausschalten

Leistungsmerkmale im Gesprächszustand

- Rückfrage
- Makeln
- Konferenz
- Trennen und zurück zum Wartenden
- Rückruf aktivieren
- MFV-Nachwahl ermöglichen

Zur Signalisierung der Leistungsmerkmale werden System-Kennzahlen verwendet (z. B. *1 für Anrufumleitung programmieren).

INFO: Für Mobility Entry-Teilnehmer muss das Teilnehmer-Flag **DISA Berechtigung** aktiviert sein.

Bei OpenScape Business X stehen maximal 16 DTMF-Code Receiver-Ressourcen zur Verfügung, d. h. es können maximal 16 Teilnehmer (analoge, Mobility, etc.) gleichzeitig DTMF-Code-Receiver reservieren. Teilnehmer, bei denen das Flag **DTMF-basierte Leistungsmerkmalaktivierung** gesetzt ist, reservieren sich für die Dauer des Gespräches jeweils einen Code-Receiver.

Bei OpenScape Business S wird die Steuerung der Funktionen über DTMF-Codes unterstützt, wenn die DTMF-Ziffern nach RFC 2833 übertragen werden. Wird im Netzwerk ein externer Session Border Controller (SBC) genutzt, ist keine DTMF-Erkennung möglich.

Verwandte Themen

- One Number Service
- Vergleich Mobile Clients und Mobility Entry
- Abhängigkeiten für Mobile Clients und Mobility Entry

18.2.4 Vergleich Mobile Clients und Mobility Entry

Die Mobile Clients myPortal for Mobile und myPortal to go und Mobility Entry unterstützen unterschiedliche Leistungsmerkmale.

Leistungsmerkmal	myPortal for Mobile	myPortal to go	Mobility Entry
Allgemeine Funktionen			
Mobilfunkvertrag mit Datenoption	ja (Flatrate empfohlen)	ja (Flatrate empfohlen)	nein
Parallele Rufsignalisierung an Systemtelefon und Mobiltelefon (Twinning)	ja	ja	ja
Übertragung der Anrufer-Rufnummer zum Mobiltelefon (wenn das Netz externe Rufnummern als CLIP überträgt, CLIP no Screening)	ja	ja	ja
One Number Service (wenn das Netz externe Rufnummern als CLIP überträgt, CLIP no Screening))	ja	ja	ja
Anrufschutz/abschaltbare Anrufweiterleitung	nein	nein	ja
Rufnummernunterdrückung ein-/ausschaltbar	nein	nein	ja
Automatische Identifizierung registrierter Teilnehmer	ja	ja	ja
Betrieb ohne Bürotelefon (als virtueller Teilnehmer)	ja	ja	ja
Nutzbar mit Softwitch	ja	ja	nein
Anwesenheitsstatus, Journal, Sprachbox			
Eigenen Anwesenheitsstatus ändern	ja	ja	nein
Anwesenheitsstatus anderer Teilnehmer sehen	ja	ja	nein
Journal	Alle, Entgangen, Angenommen, Ankommend, Gehend	Neue, Alle, Entgangen, Angenommen, Sprachnachrichten	nein
Gemeinsame Sprachbox, Abfrage auch von unterwegs möglich	ja	ja	ja
Anzeige eingegangener Sprachnachrichten	Anzeige neuer, abgehörter und gespeicherter Sprachnachrichten	Anzeige neuer, abgehörter und gespeicherter Sprachnachrichten	nein
Wählen			
Zugriff auf Kontakte im Mobiltelefon	nein	ja	ja
Zugriff auf Kontakte im Kommunikationssystem	Externes Vezeichnis (UC Suite), internes Verzeichnis, persönliche Kontakte und Systemtelefonbuch	Externes Vezeichnis (UC Suite), internes Verzeichnis, persönliche Kontakte und Systemtelefonbuch	nein
Favoriten	ja	ja	nein
Manuelle Wahl	ja	ja	ja
Wahlwiederholung	ja	ja	nein

Leistungsmerkmal	myPortal for Mobile	myPortal to go	Mobility Entry
Wahlverfahren	Callback, Call Through, SIP, Assoziierte Wahl (nur für Tablet PC)	Callback, Call Through, Assoziierte Wahl	Callback, Call Through
Während des Gesprächs			
Rückfrage	ja	ja (nicht mit SIP-Telefon)	ja
Makeln	ja	ja (nicht mit SIP-Telefon)	ja
Vermitteln	ja	ja (nicht mit SIP-Telefon)	ja
Konferenz	ja	ja (nicht mit SIP-Telefon)	ja
Rückruf bei Frei und Besetzt	nein	nein	ja
Gesprächsübernahme vom Mobiltelefon auf das Systemtelefon	ja	ja	ja
Besetztanzeige auch bei Gesprächen am Mobiltelefon (bei One Number Service)	ja	ja	ja

Verwandte Themen

- myPortal for Mobile
- Mobility Entry

18.2.5 Abhängigkeiten für Mobile Clients und Mobility Entry

Die Mobile Clients myPortal for Mobile und myPortal to go und Mobility Entry besitzen Abhängigkeiten zu anderen Leistungsmerkmalen (z. B. zu DISA).

Abhängigkeit	myPortal for Mobile	myPortal to go	Mobility Entry
DISA-Rufnummer	Beim Wahlmodus Mobile Callback muss die DISA-Rufnummer konfiguriert sein.		
Externe Zielrufnummer	Die Anwahl von externen Zielrufnummern durch den mobilen Teilnehmer wird aufgrund der LCR-Konfiguration im System gesteuert. Sie kann damit über das ISDN-Festnetz, analoge Festnetz oder über ITSP erfolgen.		
CLIP no Screening aktivieren	Um beim mobilen Teilnehmer die Nummer eines Anrufers anzeigen zu können, muss sie vom Netzanbieter ungeprüft durchgereicht werden.		
CLIP des mobilen Teilnehmers	Die CLIP des mobilen Teilnehmers muss zum Kommunikationssystem übertragen werden. Der Netzanbieter muss diese zur Verfügung stellen.		
LCR-Administration	Da manche Netzanbieter (Festnetz oder ITSP) Zielrufnummern mit eigenem internationalen Präfix nicht akzeptieren, muss vom System die Zielrufnummer um diesen Präfix gekürzt werden. Dies kann bei der Leitweglenkung (LCR) administriert werden.		
B-Kanäle/Externverbindungen	Die Anzahl der B-Kanäle ist abhängig von der Verbindungsdauer bzw. der Anzahl mobiler Teilnehmer. Jede von Extern kommende Verbindung zu einem mobilen Teilnehmer erfordert im System 2 Sprachkanäle. Falls zu wenig Sprachkanäle zur Verfügung stehen, ist die Erreichbarkeit des mobilen Teilnehmers nicht gewährleistet und der mobile Teilnehmer kann selbst keine Anrufe mit One Number Service tätigen.		

Abhängigkeit	myPortal for Mobile	myPortal to go	Mobility Entry
Notrufnummern	Wenn ein mobiler Teilnehmer eine Notrufnummer über das Kommunikationssystem wählt, kann der Standort seines Mobiltelefons nicht ermittelt werden. Es ist empfehlenswert, eine Notrufnummer direkt zu wählen.		
Anwahl interner Rufnummern	Bei Anwahl interner Rufnummern durch den mobilen Teilnehmer im internationalen Format (z. B. 0004989100) muss die Standortnummer des Kommunikationssystems konfiguriert sein. Ansonsten werden interne Ziele über Amt angewählt und damit entstehen Kosten.		
Pflege von Verzeichnissen	Um in allen Wahlmodi die Erreichbarkeit von Gesprächspartnern bei der Wahl aus Verzeichnissen sicherzustellen, sollten alle externen Rufnummern im kanonischen Format (z. B. +49 89 100) eingetragen sein.	Um in allen Wahlmodi die Erreichbarkeit von Gesprächspartnern bei der Wahl aus Verzeichnissen sicherzustellen, sollten alle externen Rufnummern im kanonischen Format (z. B. +49 89 100) eingetragen sein.	-
Firewall	Es wird ein Datenkanal zum integrierten Web-Server des Kommunikationssystems aufgebaut. Deshalb muss in der Firewall eine Portweiterleitung auf Port 8801 (http) bzw. Port 8802 (https) eingerichtet sein. Es wird jedoch empfohlen keine Portweiterleitung für Port 8803 (https) für den Zugriff auf UC Smart Assistant zu konfigurieren.	Es wird ein Datenkanal zum integrierten Web-Server des Kommunikationssystems aufgebaut. Deshalb muss in der Firewall eine Portweiterleitung auf Port 8801 (http) bzw. Port 8802 (https) eingerichtet sein. Es wird jedoch empfohlen keine Portweiterleitung für Port 8803 (https) für den Zugriff auf UC Smart Assistant zu konfigurieren.	-
Datenverbindung	Es wird empfohlen einen Mobilfunkvertrag mit Datenflatrate abzuschließen. Nutzer von Volumentarifen sollten in den Einstellungen von myPortal for Mobile die Option "Automatisches Refresh" ausschalten.	Es wird empfohlen einen Mobilfunkvertrag mit Datenflatrate abzuschließen. Nutzer von Volumentarifen sollten in den Einstellungen von myPortal for Mobile die Option "Automatisches Refresh" ausschalten.	-
Parallele Verbindungen	Für einige Leistungsmerkmale ist eine gleichzeitige Spach- und Datenverbindung erforderlich. Dies muss sowohl vom Mobilfunknetzbetreiber, als auch vom mobilen Endgerät unterstützt werden.	Für einige Leistungsmerkmale ist eine gleichzeitige Spach- und Datenverbindung erforderlich. Dies muss sowohl vom Mobilfunknetzbetreiber, als auch vom mobilen Endgerät unterstützt werden.	-
Verbindungsaufbau vom Kommunikationssystem zum mobilen Teilnehmer über	Alle Leitungstypen	Alle Leitungstypen	Alle Leitungstypen, die DTMF-Übertragung unterstützen.

Verwandte Themen

- myPortal for Mobile

- Mobility Entry

18.2.6 One Number Service

Über den One Number Service (ONS) wird das Mobiltelefon zur Festnetz-Nebenstelle. Der Teilnehmer ist unter einer Rufnummer weltweit erreichbar und identifiziert sich nur noch mit seiner Festnetzrufnummer.

Durch Einrichtung einer Teamschaltung ist One Number Service mit einer gemeinsamen Rufnummer für Büroarbeitsplatz (Systemtelefon) und Mobiltelefon möglich. Der Anrufer wählt die Rufnummer des Systemtelefons (Festnetz). Gehende Anrufe vom Mobiltelefon werden dem Angerufenen mit der Festnetzrufnummer signalisiert. Ein weiterer Vorteil des One Number Services ist die Besetztanzeige für den mobilen Teilnehmer.

Verwandte Themen

- myPortal for Mobile
- Mobility Entry

18.2.7 Dual-Mode-Telefonie

Dual-Mode-Mobiltelefone unterstützen einerseits GSM/UMTS-Netze und andererseits WLAN-Netze. Über WLAN ist eine Registrierung als SIP-Teilnehmer am Kommunikationssystem möglich.

Befindet sich das Dual-Mode-Mobiltelefon in WLAN-Reichweite, wird es automatisch als SIP-Teilnehmer gerufen (SIP-Leistungsmerkmale). Außerhalb der WLAN-Reichweite wird das Dual-Mode-Mobiltelefon über GSM/UMTS gerufen (Mobiltelefon-Integration-Leistungsumfang möglich).

Das automatische Weiterleiten an die GSM-Rufnummer funktioniert nur dann, wenn der zugehörige SIP-Teilnehmer im System als Mobiltelefon-Teilnehmer eingetragen ist (Mobiltelefon Integration). Das bedeutet, wenn der SIP-Teilnehmer registriert ist, wird er als SIP-Teilnehmer gerufen, wenn nicht, dann wird er über die in der Mobiltelefon-Integration-Konfiguration zugeordnete GSM-Rufnummer gerufen. CTI-Anruffunktionen sind für SIP-Clients nicht in myPortal for Mobile verfügbar, stattdessen erfolgt die Steuerung gegebenenfalls innerhalb des SIP-Clients (siehe auch Freigabemitteilung und `http://wiki.unify.com`).

Die Gespräche laufen auf dem Firmengelände über WLAN. Solange über WLAN telefoniert wird, fallen auf dem Mobiltelefon keine Gesprächsgebühren an. Handover und Roaming werden innerhalb der WLAN-Reichweite unterstützt (wenn die WLAN-Infrastruktur dafür ausgelegt ist), nicht jedoch von WLAN nach GSM und umgekehrt.

18.2.8 Konfiguration von myPortal for Mobile und Mobility Entry

myPortal for Mobile und Mobility Entry werden mit dem Wizard **Mobiltelefon Integration** konfiguriert.

Mit dem Wizard **Mobiltelefon Integration** kann der Administrator:

- One Number Service einrichten
- myPortal for Mobile einrichten
- Mobility Entry einrichten
- Dual-Mode-Telefone einrichten

Die Mobiltelefon-Integration von GSM-Telefonen erfolgt über virtuelle Teilnehmer. Damit werden Leistungsmerkmale auf den mobilen Teilnehmer übertragen. Jedem Teilnehmer mit einer entsprechenden Lizenz (Mobility User) kann maximal ein mobiler Teilnehmer zugeordnet werden

Betriebsmode von Mobiltelefonen

Es sind folgende Betriebsmodi für Mobiltelefone realisiert:

- **GSM Mode**
  Ein Anruf der internen mobilen Rufnummer wird am GSM-Mobiltelefon signalisiert.
- **WLAN Mode**
  Ist das WLAN-Mobiltelefon über WLAN erreichbar, wir der Anruf über WLAN geführt. Ist das WLAN nicht erreichbar, wird der Anruf über GSM geführt.

Twinning

Ein Anruf wird parallel am Mobiltelefon und am Systemtelefon signalisiert (Twinning). Um Twinning zu realisieren muss nach Konfiguration der **Mobiltelefon Integration** eine Teamschaltung konfiguriert werden. Verwenden Sie dazu den Wizard **Teamschaltung** und wählen als erstes Telefon die Rufnummer aus, unter der die Parallelsignalisierung erfolgen soll (z. B. das Systemtelefon). Für die Nutzung von myPortal for Mobile wird als letzter Schritt im Wizard **Mobiltelefon Integration** der Benutzername auf die Team-Gruppe umkonfiguriert. Auf dem Systemtelefon kann für die unterbrechungsfreie Übernahme von Mobiltelefongesprächen eine Direktruftaste zu dem Mobility-Teilnehmer programmiert werden. Der volle Funktionsumfang wird mit Systemtelefonen (HFA) erreicht. SIP- Telefone können mit Einschränkungen verwendet werden, sie unterstützen z. B. keine MULAP-Taste.

Verwandte Themen

- Konfiguration von Teamschaltungen / Team-Gruppen und Chef/Sekretär-Funktionen / Top-Gruppen über Wizards

18.2.8.1 Wie Sie ein GSM-Mobiltelefon integrieren

Mit dem Wizard **Mobiltelefon Integration** integrieren Sie Mobiltelefone in das Kommunikationssystem.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

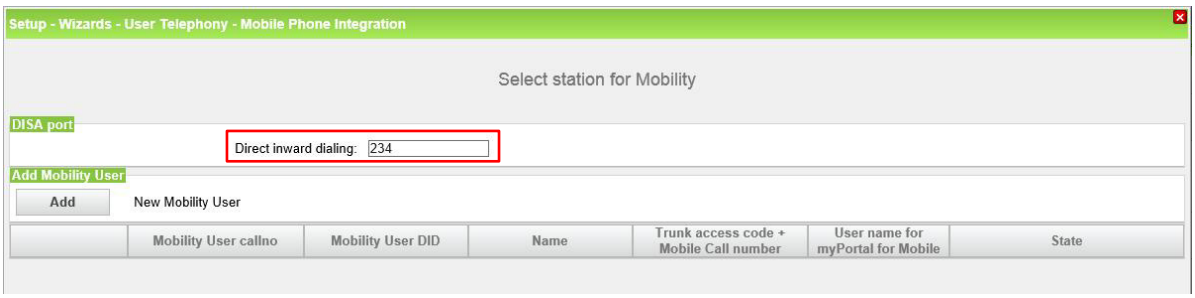
Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > User-Telefonie**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Mobiltelefon Integration** zu starten. Das Fenster **Teilnehmer für Mobility auswählen** wird angezeigt.

4) Wählen Sie bei **DISA Zugang** die **Durchwahl**-Nummer aus (oder geben Sie sie ein), unter der sich mobile Teilnehmer in das Kommunikationssystem einwählen können.



> ***INFO:*** DISA ist erforderlich für Mobilty Entry (Steuerung des Systems über DTMF) und für myPortal for Mobile (nur bei Verwendung von Call-Through).

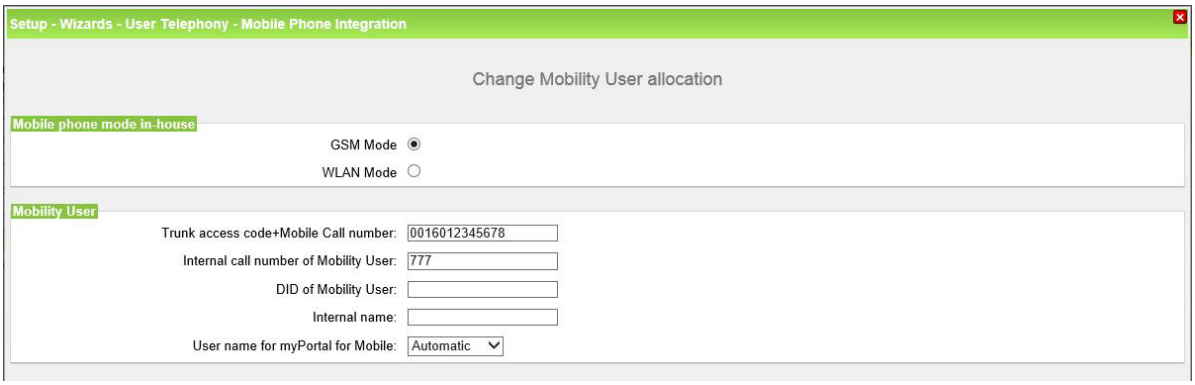
5) Klicken Sie auf **Hinzufügen** bzw. **Bearbeiten** des entsprechenden Teilnehmers, dessen GSM-Mobiltelefon Sie ins Kommunikationssystem integrieren wollen. Das Fenster **Mobility Teilnehmer zuweisen** wird angezeigt.

6) Wählen Sie **GSM Mode** als Handybetriebsmode aus.

7) Geben Sie unter **Kennzahl zur Amtsholung+Mobile Rufnummer** die Rufnummer des Mobiltelefons ein (z. B. 0016012345678) ein.

8) Geben Sie die **Interne Rufnummer des Mobility-Teilnehmers** (z. B. 777), einen beliebigen **internen Namen** und die **Durchwahlnummer** ein. Beachten Sie, dass die interne Rufnummer noch nicht vergeben sein darf.

9) Wählen Sie in der Aufklappliste **Benutzername für myPortal for Mobile** den Eintrag **Automatisch** aus (bei Auswahl von Automatisch wird als Benutzername die interne Rufnummer des Teilnehmers vergeben).



10) Nur bei UC Smart: Ordnen Sie bei Bedarf dem Teilnehmer eine Mailbox zu:

a) Wählen Sie in der Aufklappliste **Mailboxtyp UC Smart** aus, ob der Teilnehmer eine Standardmailbox oder eine Vermittlungsmailbox (AutoAttendant) erhalten soll.

b) Nur bei Standardmailbox: Wenn ein Anrufer eine Nachricht auf der Sprachbox hinterlassen darf, aktivieren Sie das Kontrollkästchen **Aufnahme**.

c) Wählen Sie aus der Aufklappliste **Begrüßung** eine Begrüßung aus.

d) Wenn das Kennwort der Sprachbox zurückgesetzt werden soll, aktivieren Sie das Kontrollkästchen **Passwort Reset**.

INFO: Das Kontrollkästchen **Passwort Reset** muss bei einer Neueinrichtung einer Sprachbox nicht gesetzt sein. Es bewirkt das Rücksetzen des Kennworts der Sprachbox. Bei einer Neueinrichtung muss der Teilnehmer sowieso beim ersten Zugriff auf seine Sprachbox das Initial-Kennwort ändern.

---

11) Klicken Sie auf **OK & Weiter**.

12) Klicken Sie auf **OK & Weiter** und abschließend auf **Beenden**.

18.2.8.2 Wie Sie ein Dual-Mode-Telefon (GSM/WLAN) mit SIP-Client integrieren

Mit dem Wizard **Mobiltelefon Integration** konfigurieren Sie ein Mobiltelefon als Dual-Mode-Telefon mit SIP-Client (WLAN Mode).

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

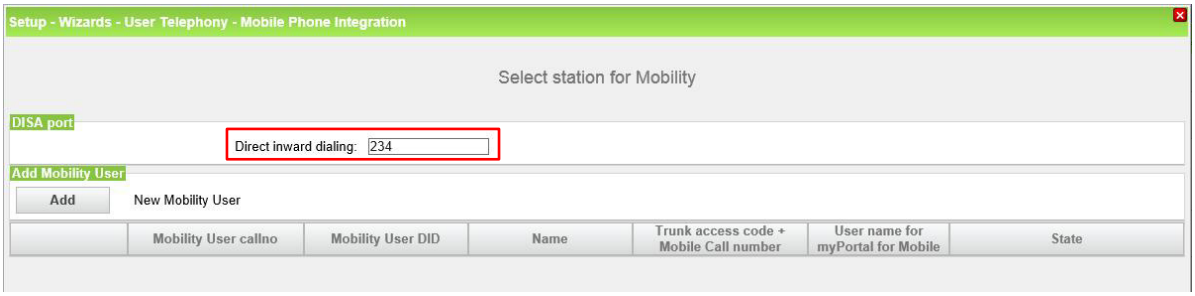
Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > User-Telefonie**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Mobiltelefon Integration** zu starten. Das Fenster **Teilnehmer für Mobility auswählen** wird angezeigt.

4) Wählen Sie bei **DISA Zugang** die **Durchwahl**-Nummer aus (oder geben Sie sie ein), unter der sich mobile Teilnehmer in das Kommunikationssystem einwählen können.



> ***INFO:*** DISA ist erforderlich für Mobilty Entry (Steuerung des Systems über DTMF) und für myPortal for Mobile (nur bei Verwendung von Call-Through).

5) Klicken Sie auf **Hinzufüge**n bzw. **Bearbeiten** des entsprechenden Teilnehmers, dessen GSM-Mobiltelefon Sie ins Kommunikationssystem integrieren wollen. Das Fenster **Mobility Teilnehmer zuweisen** wird angezeigt.

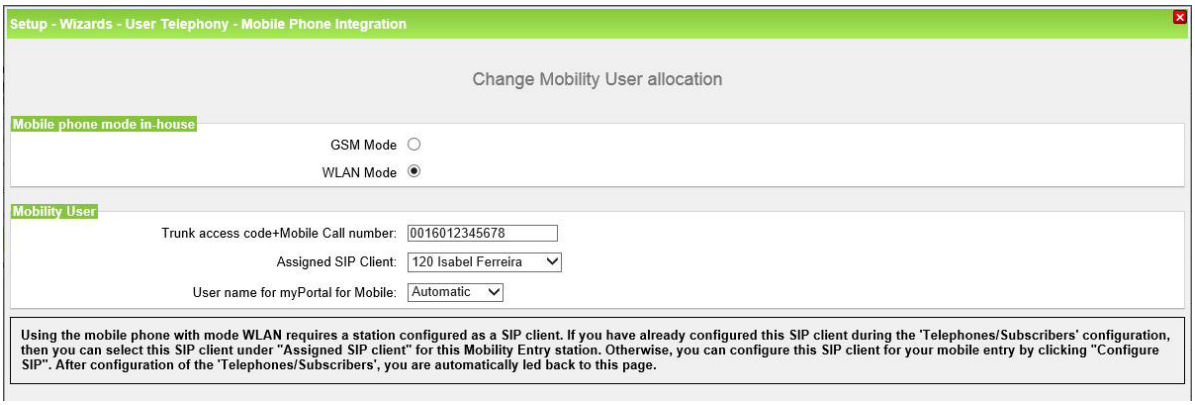
6) Wählen Sie **WLAN Mode** als Handybetriebsmode aus.

7) Geben Sie unter **Kennzahl zur Amtsholung+Mobile Rufnummer** die Rufnummer des Mobiltelefons ein (z. B. 0016012345678) ein.

8) Wählen Sie aus der Aufklappliste den **Zugeordneten SIP-Client** aus.

Wenn der SIP-Client noch nicht konfiguriert ist, klicken Sie auf **SIP konfigurieren** und richten Sie einen SIP-Client ein. Nach der SIP-Teilnehmer-Konfiguration werden Sie automatisch auf diese Seite zurück geführt.

9) Wählen Sie in der Aufklappliste **Benutzername für myPortal for Mobile** den Eintrag **Automatisch** aus (bei Auswahl von Automatisch wird als Benutzername die interne Rufnummer des Teilnehmers vergeben).



10) Klicken Sie auf **OK & Weiter**.

11) Klicken Sie auf **OK & Weiter** und abschließend auf **Beenden**.

18.2.8.3 Wie Sie die Web-Schnittstelle für Mobiltelefone und Web-Clients aktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Aktivieren Sie Web Services als Voraussetzung für folgende Leistungsmerkmale:

- Mobiltelefon-Integration
- Application Launcher

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Wenn Sie UC Smart verwenden, klicken Sie im Navigationsbaum auf **Applikationen > UC Smart > Grundeinstellungen**.

3) Prüfen Sie, ob UC Smart **Aktiv** ist.

4) Wenn Sie Web Services für Mobiltelefone aktivieren möchten, wählen Sie mindestens eine der folgenden Möglichkeiten:

- Wenn Sie verschlüsselte Verbindungen erlauben möchten, aktivieren Sie das Kontrollkästchen **HTTPS**.
- Wenn Sie unverschlüsselte Verbindungen erlauben möchten, aktivieren Sie das Kontrollkästchen **HTTP**.



INFO: Aus Sicherheitsgründen wird dringend empfohlen, bei Nutzung von myPortal for Mobile/Tablet über Internet nur eine verschlüsselte Verbindung (HTTPS) zu nutzen.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

18.2.8.4 Wie Sie die Mobiltelefon-Integration löschen

Mit dem Wizard **Mobiltelefon Integration** löschen Sie die Integration des Mobiltelefons.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > User-Telefonie**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Mobiltelefon Integration** zu starten. Das Fenster **Teilnehmer für Mobility auswählen** wird angezeigt.

4) Klicken Sie auf **Bearbeiten** des entsprechenden Teilnehmers, den Sie löschen wollen. Das Fenster **Mobility Teilnehmer zuweisen** wird angezeigt.

5) Klicken Sie im Fenster unten auf **Daten löschen**.

6) Klicken Sie auf **OK & Weiter**.

7) Klicken Sie auf **OK & Weiter** und abschließend auf **Beenden**.

18.3 Mobilität im Büro

Mobilität im Büro wird erreicht über DeskSharing, Cordless-Telefone und WLAN-Telefone. Für DeskSharing werden mit IP-Mobility (Mobiles Logon und Flex Call) Leistungsmerkmale für mobile Teilnehmer angeboten, die das Telefon an einem fremden Arbeitsplatz wie ihr eigenes nutzen möchten.

18.3.1 DeskSharing

Mit DeskSharing können sich mehrere Teilnehmer ein Systemtelefon und damit ein IP-Telefon (HFA) teilen.

Beim DeskSharing hat der Teilnehmer keinen festen Arbeitsplatz und kein festes Bürotelefon. DeskSharing ermöglicht es mehreren mobilen Teilnehmern des Kommunikationssystems sich einen Büroarbeitsplatz bzw. das Telefon zu teilen. Der Teilnehmer loggt sich an dem Telefon an dem Arbeitsplatz ein, an dem er gerade arbeitet.

Nach dem Anmelden wird die Rufnummer des Teilnehmers für das benutzte Systemtelefon übernommen. Das Systemtelefon kann nicht mehr unter seiner ursprünglichen Rufnummer erreicht werden. Meldet sich der Teilnehmer an einem weiteren Systemtelefon an, wird die Rufnummer auf dieses neue Systemtelefon übertragen. Nach dem Abmelden (Ausloggen) loggt sich das Systemtelefon automatisch wieder mit seiner eigenen nicht-mobilen-Nummer an.

Zur Aktivierung ist einer der folgenden Schritte am Systemtelefon durchzuführen:

- Kennzahl für Mobiles Logon + Nummer des mobilen Teilnehmers + optionales Kennwort/PIN

Bei der Verwendung von Telefonen mit unterschiedlicher Anzahl von Funktionstasten können sich Einschränkungen bei der Übernahme des Tastenlayouts ergeben.

Wenn DeskSharing für IP-Telefone (HFA) in vernetzten Knoten realisiert werden soll, muss ein externer DLS (Deployment Service) installiert werden. Hierzu wird das notwendige Fachwissen vorausgesetzt.

Folgende Leistungsmerkmale können bei DeskSharing genutzt werden:

- Direktansprechen (Paging)
- Konferenz
- Aufschalten
- Makeln
- Parken
- Rückfrage
- Übergeben
- Anrufübernahme
- Anrufschutz
- Anrufumleitung
- Info Senden (Message Waiting)
- Rückruf
- Rufnummernunterdrückung
- Rufzuschaltung

INFO: Für jede mobile Rufnummer wird eine zusätzliche Deskshare-Lizenz benötigt. Diese Deskshare-Lizenz muss für die entsprechenden Teilnehmer aktiviert werden und der Teilnehmer muss als **mobil** konfiguriert und Relocate/Rufnummerntausch muss aktiviert sein.

Ein Systemtelefon, das für DeskSharing verwendet wird, benötigt nicht zwingend eine Lizenz. Wenn keine Lizenz aktiviert ist und kein DeskSharing-Teilnehmer angemeldet ist, sind aber auch keine Notrufe von diesem Telefon aus möglich. Das Systemtelefon/Teilnehmer muss als **nicht mobil** konfiguriert sein.

Wenn ein Systemtelefon nicht für DeskSharing verwendet werden soll, muss es als **nicht mobil und blockiert** eingerichtet sein.

18.3.2 Integrierte Cordless-Lösung

OpenScape Business Cordless ist die integrierte Cordless-Lösung zum Betrieb von Cordless-Telefonen (DECT-Telefonen) über das Kommunikationssystem. Mit

den angeschlossenen DECT-Telefonen können die HFA-Leistungsmerkmale von OpenScape Business genutzt werden.

Bei der integrierten Cordless-Lösung sind die DECT-Telefone interne, systemspezifische Teilnehmer, im Gegensatz zu separaten DECT-Anlagen, die über Standardschnittstellen angeschaltet werden.

Die Anschaltung der OpenScape Business Basisstationen für den Betrieb der DECT-Telefone kann realisiert werden über:

- für OpenScape Business X1/X3/X5: Anschaltung direkt an die $U_{P0/E}$-Schnittstellen des Mainboards des Kommunikationssystems (DECT Light)
- für OpenScape Business X3/X5: Anschaltung an die $U_{P0/E}$-Schnittstellen einer SLU8N/SLU8NR-Baugruppe
- für OpenScape Business X5W/X8: Anschaltung an die $U_{P0/E}$-Schnittstellen einer Cordless-SLC-Baugruppe

Die Cordless-Funktechnologie entspricht dem DECT-Standard (Digital Enhanced Cordless Telecommunications). Der gesamte, vom System verwaltete Funkbereich besteht aus Basisstationen, die entweder zusammen ein lückenloses Netz sich überschneidender Funkzellen oder einzelne Funkinseln bilden. Die Größe einer Funkzelle ist abhängig von den örtlichen/baulichen Gegebenheiten.

ECO Mode

Im ECO Mode (Economic Mode) wird die Sendeleistung der DECT-Telefone entweder um einen fest eingestellten Wert (statisch) gesenkt oder jedes DECT-Telefon passt seine Sendeleistung selbstständig an die empfangene Signalstärke an (adaptiv). Der ECO Mode kann am Kommunikationssystem für alle DECT-Telefone systemweit aktiviert werden (**Experten-Modus > Telephonie > Cordless > Systemweit**). Eine Konfiguration an den DECT-Telefonen ist nicht notwendig.

- Statische Sendeleistungsanpassung
  Die DECT-Telefone und die Basisstation senken die Sendeleistung auf einen fest eingestellten Wert ab.
- Adaptive Sendeleistungsanpassung
  Die DECT-Telefone senden abhängig von der jeweiligen Empfangsfeldstärke mit normaler oder mit reduzierter Sendeleistung. Bei Handover wird zuerst auf die hohe Sendeleistung geschaltet und anschließend abhängig vom Empfang die Sendeleistung reduziert.

DECT-Telefone

Die integrierte Cordless-Lösung unterstützt die Anschaltung GAP-fähiger Mobiltelefone fremder Hersteller. Der volle HFA-Leistungsumfang kann aber nur mit den freigegebenen DECT-Telefonen genutzt werden.

Konfiguration

Für die Beschreibung der Konfiguration siehe *Integrierte Cordless-Lösung*.

Baugruppen und Basisstationen

Die Beschreibung der Baugruppen und Basisstationen finden Sie in der Servicedokumentation (*integrierte Cordless-Lösung*).

18.3.2.1 Cordless-Direktanschaltung (DECT Light)

Bei der Direktanschaltung (auch als DECT Light bezeichnet) wird die Basisstation direkt an eine $U_{P0/E}$-Schnittstelle des Mainboards des Kommunikationssystems oder an eine $U_{P0/E}$-Schnittstelle einer SLU8N/SLU8NR-Baugruppe (nur für OpenScape Business X3/X5) angeschlossen.

Für die Anschaltung von Basisstationen an eine SLU8N/SLU8NR-Baugruppe nur für OpenScape Business X3/X5) gelten folgende Anschaltbedingungen:

- Insgesamt können maximal 15 Basisstationen (7 am Mainboard und weitere 8 an einer SLU8N/SLU8NR-Baugruppe) betrieben werden. Die max. Anzahl der anschließbaren DECT-Telefone bleibt unverändert bei 32.
- Es kann nur eine SLU8N/SLU8NR-Baugruppe für die Anschaltung von Basisstationen verwendet werden.
- Für den Anschluss der Basisstation an eine $U_{P0/E}$-Schnittstelle der SLU8N/SLU8NR-Baugruppe kann nur der erste Port der Basisstation verwendet werden. Die zweite Port der Basisstation wird nicht für den Anschluss an eine weitere $U_{P0/E}$-Schnittstelle unterstützt.
- Die $U_{P0/E}$-Schnittstellen der SLU8N/SLU8NR-Baugruppe können gemischt mit Basisstationen oder Telefonen beschaltet werden.
- Mit einem zusätzlich installierten CMA-Modul können bis zu 4 gleichzeitige Gespräche pro Basisstation geführt werden.

Für die DECT-Telefone werden TDM User Lizenzen benötigt.

18.3.2.2 Cordless-Baugruppenanschaltung

Bei der Baugruppenanschaltung werden die Basisstationen an die $U_{P0/E}$-Schnittstellen der Cordless-Baugruppen (SLC-Baugruppen) angeschlossen.

Basisstationen können an die $U_{P0/E}$-Schnittstellen folgender Cordless-Baugruppen angeschlossen werden:

- SLC16N bei OpenScape Business X5W (nur Wandsystem)
- SLCN bei OpenScape Business X8

Bis zu vier Cordless-Baugruppen (SLCN) können in OpenScape Business X8 eingesetzt werden. Über alle vier Cordless-Baugruppen steht die volle Cordless-Funktionalität (Roaming und Seamless Connection Handover) zur Verfügung, da die Funkfelder der Cordless-Baugruppen innerhalb des Kommunikationssystems über SLC-Vernetzungsleitungen synchronisiert werden (Multi-SLC). Netzweites Handover wird derzeit nicht unterstützt.

18.3.2.3 Systemausbau

In Abhängigkeit vom Kommunikationssystem können bis zu 64 Basisstationen angeschlossen und bis zu 250 DECT-Telefone genutzt werden.

Die folgende Tabelle zeigt den maximal möglichen Systemausbau der integrierten Cordless-Lösung und informiert, in welchen Fällen analoger Amtszugang des Kommunikationssystems möglich ist.

HINWEIS: Die Basisstationen BS3/1 (S30807-H5482-X), BS3/3 (S30807-H5485-X) und BS3/S (X30807-X5482-X100) befinden sich im Produktauslauf und können nicht mehr bestellt werden. Der Anschluss an die Kommunikationssysteme OpenScape Business X ist aber weiterhin möglich.

Im Falle eines Defekts sind die aktuellen Basisstationen einzusetzen.

OpenScape Business	Cordless-Baugruppe	CMA erforderlich	Max. Anzahl Basisstationen beim Anschluss über 1 x $U_{P0/E}$				Max. Anzahl gleichzeitiger Gespräche pro Basisstation in Abhängigkeit vom $U_{P0/E}$-Anschluss				Max. Anzahl DECT-Telefone	Analoger Amtszugang möglich
			BS3/1	BS3/S	BS3/3	BS4	BS3/1	BS3/S	BS3/3	BS4		
X1	–	nein	7	1	–	7	2 (1 x $U_{P0/E}$)	2 (1 x $U_{P0/E}$)	–	2 (1 x $U_{P0/E}$)	14	nein
	–	ja	7	1	–	7	4 (1 x $U_{P0/E}$)	–	–	4 (1 x $U_{P0/E}$)	16	nein
X3R/X3W/ X5R/X5W	–	nein	15	1	–	15	2 (1 x $U_{P0/E}$)	2 (1 x $U_{P0/E}$)	–	2 (1 x $U_{P0/E}$)	32	nein
	–	ja	15	1	–	15	4 (1 x $U_{P0/E}$)	–	–	4 (1 x $U_{P0/E}$)	32	ja
X5W	1 x SLC16N	nein	16	–	16	16	4 (1 x $U_{P0/E}$)	–	12 (3 x $U_{P0/E}$)	12 (3 x $U_{P0/E}$)	64	ja
X8	4 x SLCN	nein	64	–	64	64	4 (1 x $U_{P0/E}$)	–	12 (3 x $U_{P0/E}$)	12 (3 x $U_{P0/E}$)	250	ja

18.3.2.4 Cordless/DECT-Telefone

Mit Stecken der SLC-Baugruppe und Eingabe der DECT-Systemkennung werden 16 Mobilteile eingerichtet. Die Mobilteil-Codes (PIN) werden vergeben und die Mobilteile können angemeldet werden. Weitere zu nutzende Mobilteile müssen erst freigeschaltet werden.

Wird im Servicefall ein Mobilteil ausgetaucht, muss vor Anmeldung des Austauschgerätes die PIN geändert werden. Beim Austausch ist grundsätzlich im

Kommunikationssystem für den betreffenden Teilnehmer eine neue PIN zu vergeben. Dadurch wir das Mobilteil automatisch abgemeldet. Und zur Sicherheit ist es nicht mehr möglich, in Kenntnis der alten PIN, ein Mobilteil missbräuchlich anzumelden.

18.3.3 Konfiguration der integrierten Cordless-Lösung

Die Konfiguration der integrierten Cordless-Lösung umfasst die Einrichtung der Basisstationen und die Anmeldung der DECT-Telefone/Mobilteile am Kommunikationssystem.

Die Konfiguration erfolgt über den Experten-Modus.

Die Voraussetzungen wie Projektierung, Ausleuchtung, Montage und Verkabelung, Aufstellen des Systems und Stecken der SLC- oder CMA-Baugruppen sind abgeschlossen (siehe auch Servicedokumentation). Die DECT-Telefone sind aufgeladen. Die DECT-Systemkennung ist bekannt. Informationen über Teilnehmer, Rufnummern, Namen und ggf. deren Zuordnung zur SLC-Baugruppe liegen vor.

Genereller Ablauf zur Konfiguration der integrierten Cordless-Lösung

1. DECT-Systemkennung eingeben und ggf. weitere Cordless-Parameter konfigurieren
2. Cordless-Basisstationen konfigurieren
3. DECT-Telefone an Cordless anmelden
4. Bei Bedarf weitere DECT-Telefone hinzufügen

Nach der Inbetriebnahme der DECT-Telefone können Rufnummer und Name und weitere Einstellungen der DECT-Teilnehmer über das WBM über den Wizard **Endgeräte/Teilnehmer** geändert werden.

DECT-Systemkennung

Die DECT-Systemkennung dient zur Unterscheidung der einzelnen DECT-Systeme und somit zur Kennzeichnung der Funksignale. Erst dadurch wird die Synchronisation der angemeldeten Mobilteile auf das System ermöglicht.

Die DECT-Systemkennung ist eine 8-stellige, hexadezimale Ziffernfolge und wird beim Erwerb des DECT-Systems mitgeliefert. Sie ist systemweit gültig (auch im Servicefall).

Die DECT-Systemkennung setzt sich zusammen aus:

Ziffer	Bedeutung
1. Ziffer	E/ARC (Access Right Code)
2.-5. Ziffer	EIC (Equipment Installers Code)
6.-7. Ziffer	FPN (Fixed Part Number)
8. Ziffer	FPS (Fixed Part Subscriber)

18.3.3.1 Wie Sie die DECT-Systemkennung eingeben und weitere Cordless-Parameter (systemweite Daten) konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.
- Eine OpenScape Business Basisstation ist am Kommunikationssystem angeschlossen.
- Die bei der Bestellung des DECT-Systems mit ausgelieferte 8-stellige DECT-Systemkennung ist vorhanden.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telephonie > Cordless**.

3) Klicken Sie im Menübaum auf **Cordless > Systemweit**.

4) Geben Sie unter **Systemkennung** die 8-stellige DECT-Systemkennung ein.

5) Ändern Sie die systemweiten Einstellungen unter Echo Handling und Economic Mode nur bei Bedarf. Eine Erklärung zu den Einstellungen finden Sie unter *Cordless > Systemweit*.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

18.3.3.2 Wie Sie Cordless-Basisstationen konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.
- Eine OpenScape Business Basisstation ist am Kommunikationssystem angeschlossen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telephonie > Cordless**.

3) Klicken Sie im Menübaum auf **Cordless > Basisstationen**. Es werden alle angeschlossenen Basisstationen angezeigt.

4) Falls eine oder mehrere Basisstationen direkt (ohne SLC-Baugruppe) am System angeschlossen sind (SLUC), können Sie die Basisstationen über die Auswahlliste **Typ** aktivieren oder deaktivieren:

a) **Basisstation**: Die Basisstation wird aktiviert und es werden automatisch 16 DECT-Telefone und eine SLC-Vernetzungsleitung vorkonfiguriert.

b) **Kein Port**: Die Basisstation wird deaktiviert mit allen zugehörigen DECT-Telefonen und der SLC-Vernetzungsleitung.

5) Ändern Sie bei Bedarf unter **Name** den vorkonfigurierten Namen der Basisstation (z. B. `Basis 1`).

6) Legen Sie unter **Pegel** den Pegel für die Basisstation fest (50% oder 100%).

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

18.3.3.3 Wie Sie DECT-Telefone erstmalig konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.
- Eine OpenScape Business Basisstation ist am Kommunikationssystem angeschlossen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telephonie > Cordless**.

3) Klicken Sie im Menübaum auf **Cordless > SLC**. Es werden alle bereits konfigurierten DECT-Telefone angezeigt. Beim Anschluss einer Basisstation werden automatisch 16 DECT-Telefone vorkonfiguriert.

4) Ändern Sie bei Bedarf unter **Rufnr.** die vorkonfigurierte interne Rufnummer des DECT-Telefons.

5) Ändern Sie bei Bedarf unter **DuWa** die vorkonfigurierte Durchwahlnummer des DECT-Telefons.

6) Ändern Sie bei Bedarf unter **Name** den vorkonfigurierten Namen des DECT-Telefons.

7) Ändern Sie bei Bedarf unter **Mobilcode** den vorkonfigurierten Mobilcode (PIN) des DECT-Telefons. Dieser Code muss am DECT-Telefon eingegeben werden bei der erstmaligen Anmeldung an der Basisstation.

8) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Verwandte Themen

- Wie Sie DECT-Teilnehmer konfigurieren

18.3.3.4 Wie Sie ein DECT-Telefon (OpenStage/Gigaset-Mobilteil) an Cordless anmelden

Vor Anmeldung eines DECT-Telefons müssen Sie das Anmeldefenster durch ein Systemtelefon mittels Kennzahl und Passwort öffnen. Maximal 10 Anmeldefenster können gleichzeitig geöffnet werden. Anschließend geben Sie die Rufnummern der anzumeldenden DECT-Telefone ein.

Schritt für Schritt

1) Öffnen Sie das Anmeldefenster am Kommunikationssystem:

a) Geben Sie an einem Systemtelefon die Kennzahl `*94 2 19970707` und das Passwort ein.

b) Geben Sie die Rufnummern der anzumeldenden DECT-Telefone ein.

2) DECT-Telefon anmelden. Hier am Beispiel: Mobiltelefon (Rufnummer 125) mit dem Mobiltelefon Code/PIN 11112345 (der als Mobilcode über Manager E konfiguriert ist) am DECT-Telefonsystem 2 anmelden:

a) Schalten Sie das Mobiltelefon ein, indem Sie die Auflegen-Taste länger als 1 s Drücken. Anschließend ertönt der Quittungston.

b) Führen Sie die folgenden Eingaben innerhalb einer Minute durch. Drücken Sie die Menütaste.

c) Wählen Sie eine Basis (hier `Basis 2`) aus und bestätigen Sie diese.

d) Rufen Sie das Zusatzmenü auf.

e) Wählen Sie **Anmelden** aus und bestätigen Sie die Auswahl.

f) Geben Sie die achtstellige PIN = Mobiltelefon Code (hier **11112345**) ein und bestätigen Sie diese.

g) Bei erfolgreicher Anmeldung wird (hier) **Basis 2** und zwischendurch das Klingelzeichen angezeigt.

18.3.3.5 Wie Sie weitere DECT-Telefone hinzufügen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.
- Eine OpenScape Business Basisstation ist am Kommunikationssystem angeschlossen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telephonie > Cordless**.

3) Klicken Sie im Menübaum auf **Cordless > SLC**.

4) Klicken Sie im Menübaum auf die gewünschte Baugruppe.

5) Klicken Sie auf die Registerkarte **DECT-Teilnehmer hinzufügen**.

6) Geben Sie unter **Anzahl DECT-Telefone** die Anzahl der neu hinzuzufügenden DECT-Telefone ein. Die neu hinzugefügten DECT-Telefone werden unter der Registerkarte **DECT Teilnehmer ändern** angezeigt.

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

18.3.3.6 Wie Sie DECT-Telefone löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.
- Eine OpenScape Business Basisstation ist am Kommunikationssystem angeschlossen.
- DECT-Telefone sind konfiguriert.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telephonie > Cordless**.

3) Klicken Sie im Menübaum auf **Cordless > SLC**. Es werden alle bereits konfigurierten DECT-Telefone angezeigt.

4) Markieren Sie in der Spalte **Löschen** die zu löschenden DECT-Telefone.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

18.3.3.7 Wie Sie die Multi-SLC-Parameter konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.
- Es sind mehrere SLCN-Baugruppen in der OpenScape Business X8 gesteckt.
- Eine OpenScape Business Basisstation ist am Kommunikationssystem angeschlossen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telephonie > Cordless**.

3) Klicken Sie im Menübaum auf **Cordless > Multi-SLC**.

4) Parameter der SLCN-Baugruppe ändern:

a) Ändern Sie bei Bedarf unter **SLC-Nr.** die vorkonfigurierte systemweit eindeutige ID-Nummer der SLCN- Baugruppe.

Wertebereich: 1-15,17-31,33-47,...,127. Vielfache von 16 sind nicht erlaubt.

b) Ändern Sie bei Bedarf unter **SLC-Rufnummer** die vorkonfigurierte systemweit eindeutige Rufnummer der SLC-Vernetzungsleitung der SLCN- Baugruppe.

INFO: Für jede SLC-Vernetzungsleitung wird ein interner S_0-Teilnehmer eingerichtet. Die SLC-Rufnummer entspricht der Rufnummer des internen S_0-Teilnehmers.

c) Kontrollieren Sie, dass bei dem internen S_0-Teilnehmer das Teilnehmer-Flag **Anklopfschutz ein** deaktiviert ist.

5) Wiederholen Sie bei Bedarf den Schritt 4 für die anderen SLCN-Baugruppen.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

18.3.3.8 Wie Sie die Daten zu den Basisstationen abfragen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.
- Eine OpenScape Business Basisstation ist am Kommunikationssystem angeschlossen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung > Cordless**.

3) Klicken Sie im Menübaum auf **Cordless > Basisstationen**.

4) Klicken Sie im Menübaum auf die gewünschte Basisstation. Die Daten zur Basisstation werden angezeigt. Eine Erklärung zu den Daten finden Sie unter *Cordless > Basisstationen*.

5) Sie können bis zu 10 verschiedene Frequenzkanäle gleichzeitig für eine Basisstation auswählen. Eine Erklärung zu den Frequenzkanälen finden Sie in der Tabelle unter *Cordless > Basisstationen*.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

18.3.3.9 Wie Sie den Hinweiston der Message Waiting Indication (MWI) für DECT-Telefone aktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telephonie > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **Grundeinstellungen > System > System Flags**.

4) Aktivieren Sie im Bereich **Systemflags** das Kontrollkästchen **CMI MWI Hinweiston**.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

18.3.3.10 Wie Sie den Anmeldestatus der DECT-Telefone abfragen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.
- Eine OpenScape Business Basisstation ist am Kommunikationssystem angeschlossen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telephonie > Cordless**.

3) Klicken Sie im Menübaum auf **Cordless > SLC**. Es werden alle bereits konfigurierten DECT-Telefone angezeigt.

4) In der Spalte **Aktiv** wird Ihnen zu jedem DECT-Telefon der Anmeldestatus angezeigt:
   - Grün: Mobiltelefon ist aktiv.
   - Rot: Baugruppen-Sperrschalter bei angemeldetem Mobiltelefon gesetzt.
   - Gelb: Mobiltelefon wurde durch Änderung der PIN automatisch wieder abgemeldet.
   - Grau: An diesem Port wurde noch nie ein Mobiltelefon angemeldet.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

18.3.4 Cordless IP

Cordless IP (DECT IP) ist die optionale Cordless-Lösung als Alternative zur integrierten Cordless-Lösung oder zum Einsatz mit OpenScape Business S.

Die DECT-Telefone an Cordless IP kommunizieren über die BSIP-Basistation mit dem Kommunikationssystem wie SIP-Telefone. Mit Cordless IP können deshalb nur SIP-Leistungsmerkmale genutzt werden. Weitere Informationen zu Cordless IP siehe Dokumentation zu HiPath Cordless IP.

Für alle SIP-Teilnehmer, die an einer Cordless-IP angemeldet sind, muss der Teilnehmer-Parameter **Autom. Rufannahme, CSTA** deaktiviert sein. Ansonsten kann es dazu führen, dass Anrufe zwischen SIP-Teilnehmern über DECT IP nicht zustande kommen.

18.3.5 WLAN-Telefone und Access Points

WLAN-Telefone und Dual-Mode-Telefone ermöglichen mobile Kommunikation. Diese Telefone können in bereits vorhandene WLAN-Infrastrukturen integriert werden. Mit WLAN Access Points können Sie drahtlose Netze aufbauen und über die gleiche Infrastruktur Sprach- und Datendienste nutzen. Es wird empfohlen nur high-performance WLAN Access Points (z. B. von Enterasys) zu verwenden.

18.3.5.1 Anforderungen an das WLAN

Beim Einsatz von WLAN muss geprüft werden, ob die grundlegenden Anforderungen für Voice-over-WLAN-Einsatz erfüllt sind. Zur Umsetzung des Wireless-Anteils des Netzwerks muss ggf. eine Funkausleuchtung (Site Survey) durchgeführt werden.

Entscheidungshilfen:

- Kleine Installationen bis zu 3 AP können bei einem Standortbesuch oder durch die Bewertung eines Gebäudeplans wirkungsvoll eingestuft werden. Hier ist eine Funkausleuchtung in der Regel nicht erforderlich.
- Bei Installationen ab 4 AP ist in jedem Fall eine Funkausleuchtung durchzuführen. Dies gilt speziell bei Installationen, die sich über mehrere Gebäude oder Stockwerke innerhalb von Gebäuden erstrecken.
- Eine Funkausleuchtung ist unabhängig von der Anzahl der AP auch erforderlich, wenn es sich um eine funk-intensive (RF = radio frequency) Umgebung handelt, oder wenn die Lösung neben anderen, bereits bestehenden WLAN-Systemen existieren soll.

18.4 Mobilität zu Hause

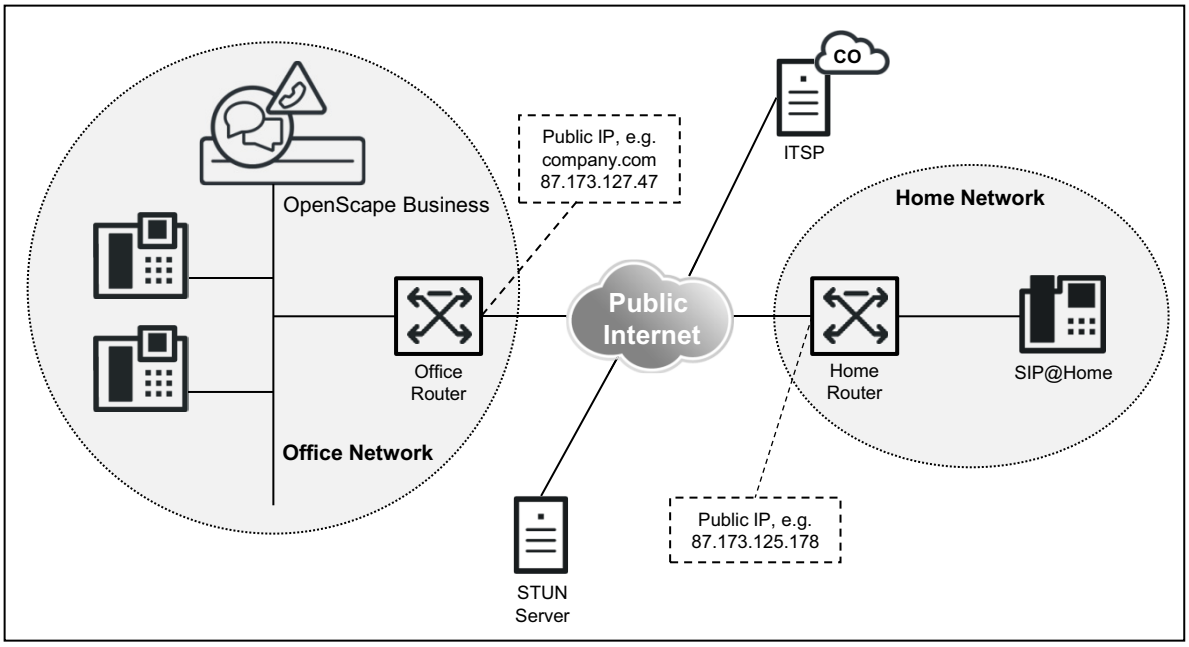
Mobilität zu Hause wird erreicht über Teleworking. Dabei können nicht-lokale Telefone (z. B. Telefon zu Hause, mobiles Telefon) in das OpenScape Business Kommunikationsnetz integriert werden.

Es gibt zwei Arten von Teleworking-Teilnehmer:

- VPN-Teilnehmer
  OpenScape Business verfügt über eine intergrierte VPN-Funktionalität. Insgesamt 10 Teleworker können gleichzeitig über VPN aktiv sein. Dabei kann es sich um einen PC zu Hause oder um ein mobiles Telefon mit Android oder iOS Betriebssystem handeln. Die VPN-Verbindung wird zwischen dem nativen VPN-Client des PCs oder des mobilen Telefons und dem OpenVPN-Server von OpenScape Business hergestellt.
  Nutzer der UC Suite können von zu Hause aus über ihren UC-Client Ihre private Telefonnummer angeben und Ihr privates Telefon wie das Bürotelefon nutzen (CallMe).

- SIP@Home-Teilnehmer
  STUN-fähige SIP-Telefone (z. B. Yealink T19) können sich über das Internet am Kommunikationssystem mit Hilfe der internen SBC-Funktion von OpenScape Business registrieren. Dazu muss das Leistungsmerkmal im WBM in den Teilnehmerdaten für jedes SIP-Telefon aktiviert werden.
  Im WBM muss zusätzlich ein STUN-Server angegeben werden, wenn kein ITSP verwendet wird oder der genutze ITSP keinen STUN-Server anbietet.
  SIP@Home unterstützt nicht die Übertragung von Video-Signalen.

Bild: SIP@Home: Komponenten



18.4.1 Konfiguration für VPN

Um Teilnehmer über die integrierte VPN-Funktionalität an das Kommunikationssystem anzuschließen, sind Konfigurationen an OpenScape Business und den VPN-Teilnehmern durchzuführen.

Konfiguration OpenScape Business

Für die VPN-Konfiguration des Kommunikationssystems siehe *Wie Sie die Anbindung von Teleworkern über VPN konfigurieren*.

Konfiguration VPN-Teilnehmer (VPN-Client)

Für die Konfiguration der VPN-Clients siehe *VPN-Clients*.

18.4.2 Konfiguration für SIP@Home

Um Verbindungen über das Internet von einem STUN-fähigen SIP-Telefon zur OpenScape Business herzustellen, sind Konfigurationen an OpenScape Business, dem Office Internet-Router und dem SIP-Telefon durchzuführen.

Konfiguration OpenScape Business

Damit sich ein SIP-Teilnehmer über das Internet am Kommunikationssystem registrieren kann, muss für den SIP-Teilnehmer die integrierte SBC-Funktion aktiviert werden (siehe *Wie Sie SIP@Home für SIP-Teilnehmer aktivieren oder deaktivieren*).

Die integrierte SBC-Funktion erkennt mit Hilfe des STUN-Protokolls die öffentliche IP-Adresse des Kommunikationssystems und den verwendeten Port. Ist das Kommunikationssystem mit einem ITSP verbunden, der einen STUN-Server anbietet, muss keine weitere Konfiguration am Kommunikationssystem vorgenommen werden. Wird aber entweder kein ITSP verwendet oder bietet der genutzte ITSP keinen STUN-Server an, muss dem Kommuniaktionssystem ein STUN-Server bekanntgegeben werden (siehe *Wie Sie einen STUN-Server für SIP@Home angeben*).

Konfiguration Office Internet-Router

Damit das SIP-Telefon das Kommunikationssystem über das Internet erreichen kann, muss im Office-Internet-Router eine Portweiterleitung für den externen SIP-Port eingerichtet werden. Um SIP-Attacken aus dem Internet zu vermeiden, muss als externer SIP-Port ein vom Standard abweichender SIP-Port verwendet werden.

Das Transport-Protokoll ist am SIP-Telefon einzustellen.

Tabelle: Portweiterleitung

Transport Protokoll	Interner SIP-Port	Externer SIP-Port	Kommentar
UDP	5060	Eingabe von z. B. 5070	Für die Portweiterleitung müssen externer und interner SIP-Port nicht gleich sein. Als externer SIP-Port kann somit ein vom internen Standard-SIP-Port 5060 abweichender Wert eingegeben werden. Daher wird UDP empfohlen.
TCP	5060 Ändern in z. B. 5080	Eingabe von z. B. 5080 (= interner SIP-Port)	Für die Portweiterleitung müssen externer und interner SIP-Port gleich sein. Um einen vom Standard-SIP-Port 5060 abweichenden externen SIP-Port zu verwenden, muss der interne SIP-Port geändert werden. Das erfordert eine Umkonfiguration aller IP-Komponenten, die SIP verwenden. Daher wird TCP **nicht** empfohlen.

Ist der Office-Internet-Router ohne feste IP-Adresse mit dem Internet verbunden, muss im Office-Internet-Router DynDNS konfiguriert sein, damit der SIP-Teilnehmer das Kommunikationssystem über das Internet erreichen kann. Über den DynDNS-Account wird die aktuelle IP-Adresse in regelmäßigen Abständen registriert. Bei kostenlosen DynDNS-Accounts, die in regelmäßigen Abständen ablaufen, kann das zeitweise zu einer Störung führen.

Konfiguration SIP-Telefon

Eine Liste aller getesteten SIP-Telefone, die STUN unterstützen, finden Sie im Internet im Unify Experts Wiki. Zu jedem freigegebenen SIP-Telefon finden Sie dort die Werte, die am SIP-Telefon eingegeben werden müssen.

Konfiguration Home-Internet-Router

Am Home-Internet-Router ist keine spezielle Konfiguration nötig.

Folgende Anforderungen muss der Home-Internet-Router erfüllen:

- Der Router muss VoIP-Funktionalität mit eingeschaltetem NAT zur Verfügung stellen (kein symmetrisches NAT).
- Die ALG-Funktion muss im Router deaktiviert sein.

Die Internet-Verbindung muss genügend Bandbreite für die Gesprächsübertragung zur Verfügung stellen. Besonders bei asymmetrischen DSL-Verbindungen ist auf genügend Upload-Bandbreite zu achten.

18.4.2.1 Wie Sie SIP@Home für SIP-Teilnehmer aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Teilnehmer**.

3) Klicken Sie im Menübaum auf **Teilnehmer > IP Clients > SIP Clients**.

4) Klicken Sie im Menübaum auf den gewünschten SIP-Teilnehmer.

5) Klicken Sie auf das Register **Workpointclient Daten ändern**.

6) Kontrollieren Sie, dass das Kontrollkästchen **Authentifizierung aktiv** aktiviert ist und ein Kennwort eingegeben ist. Die hier angegebenen Werte müssen auch am SIP-Telefon eingetragen sein.

> ***INFO:*** Bei einer Verbindung über das Internet sollte unbedingt ein sicheres Kennwort verwendet werden (mindestens 8 Zeichen inkl. Großbuchstaben, Ziffer und Sonderzeichen).

7) Wählen Sie eine der folgenden Möglichkeiten:

a) Wenn Sie SIP@Home für den gewählten SIP-Teilnehmer aktivieren möchten, aktivieren Sie das Kontrollkästchen **Internet-Registrierung am internen SBC**.

b) Wenn Sie SIP@Home für den gewählten SIP-Teilnehmer deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Internet-Registrierung am internen SBC**.

8) Schränken Sie bei Bedarf die Berechtigung des SIP-Teilnehmers ein, indem Sie auf die Registerkarte **Gruppen/RWS ändern** klicken und dort eine andere Berechtigungsgruppe für den Teilnehmer auswählen (z. B. Halbamt oder nur intern telefonieren)

9) Wenn Sie SIP@Home für weitere SIP-Teilnehmer aktivieren oder deaktivieren wollen, wiederholen Sie die Schritte 4 bis 8.

18.4.2.2 Wie Sie einen STUN-Server für SIP@Home angeben

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.
- Es wird kein ITSP verwendet oder der genutzte ITSP bietet kein STUN-Server an.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Sprachgateway**.

3) Klicken Sie im Menübaum auf **Internet-Telefonie Service Provider**.

4) Klicken Sie auf die Registerkarte **STUN-Konfiguration ändern**.

5) Geben Sie im Bereich **Default STUN Server** unter **IP-Adresse / Hostname** die IP-Adresse oder den Hostnamen des STUN-Servers ein (z. B. `stun.serviceprovider.com`).

6) Geben Sie im Bereich **Default STUN Server** unter **Port** den Port des STUN-Servers ein (z. B. `3478`).

7) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

19 Security

Security umfasst den Schutz des Kommunikationssystems und der gespeicherten und übertragenen Daten vor unbefugtem Zugriff. Dieser kann unter anderem durch Zugriffsschutz für das IP-Netz (Firewall) und verschlüsselte Übertragung (SSL, VPN) erfolgen.

Security Checklist

Das Kommunikationssystem berücksichtigt in den Voreinstellungen die Sicherheit der Kommunikation. Bei der Inbetriebnahme sind Funktionen an die individuelle Situation des Kunden anzupassen und weitere Vorkehrungen im Kundenumfeld zu treffen. Um das Bewusstsein für Sicherheitsrisiken zu schärfen und geeignete Maßnahmen zu implementieren, wird mit der Produktdokumentation eine Security Checklist bereitgestellt. Es wird dringend empfohlen, diese bei der Inbetriebnahme mit dem Kunden zu besprechen und die Maßnahmen zu dokumentieren.

19.1 Firewall

Eine Firewall ist ein System aus Software- und Hardwarekomponenten, das den Zugriff zwischen verschiedenen Netzwerken beschränkt, um ein Sicherheitskonzept umzusetzen.

Firewalls sitzen an den Schnittstellen zwischen einzelnen Netzen und kontrollieren den Datenverkehr zwischen den Teilbereichen, um ungewünschten Datenverkehr zu verhindern und nur den gewünschten Verkehr passieren zu lassen. Der häufigste Einsatz einer Firewall besteht darin, den Verkehr zwischen einem lokalen Netz (LAN) und dem Internet zu kontrollieren.

In jedem Firmennetz entkoppelt eine Firewall das interne LAN vom Internet.

Das Kommunikationssystem bietet integrierte Sicherheitsfunktionen; dabei unterscheiden sich OpenScape Business X und OpenScape Business S in der Funktionalität.

OpenScape Business X bietet folgende Leistungsmerkmale:

- Port Firewall / NAT (Firewall zwischen WAN-Port und LAN)
- Application Firewall (Firewall für den Zugang zum Kommunikationssystem)

OpenScape Business S nutzt die Linux-Firewall.

19.1.1 Porthandling

Das Porthandling dient zur Portfreischaltung (Port Mapping, Portweiterleitung) in der Firewall des integrierten Routers der OpenScape Business X.

HINWEIS: Öffnen Sie nur dann Ports, wenn es für eine bestimmte Anwendung zwingend erforderlich ist!

Ports (Services oder Dienste) sind für die Kommunikation über die Protokolle TCP und UDP erforderlich, da sie es mehreren Anwendungen ermöglichen über eine einzige Verbindung gleichzeitig Daten auszutauschen.

Unter dem Begriff Firewall versteht man im Allgemeinen eine Port-Firewall (also das Sperren einzelner Dienste/Services oder auch Ports genannt). Die Port-Firewall wirkt nur auf den WAN-Anschluss von OpenScape Business.

Bei OpenScape Business S kann man auf dem LAN-Anschluss unter Linux eine Port-Firewall aktivieren. Bei OpenScape Business X ist die Firewall auf dem WAN-Anschluss aktiv um das interne Netz (am LAN-Anschluss) vor Angriffen aus dem Internet zu schützen. Sollen trotzdem bestimmte Ports/Dienste aus dem Internet erreichbar sein (z. B. für myPortal for Mobile) müssen diese freigegeben werden (siehe Portfreigabe). Alle Ports/Dienste für die Funktionalität von OpenScape Business X sind auf dem LAN-Anschluss (zum internen Kundennetz hin) automatisch freigegeben.

OpenScape Business S besitzt nur einen LAN-Anschluss (ins interne Kunden-Netz) und wird gegenüber dem Internet durch andere Komponenten/Router im Kundennetz geschützt. Zusätzlich ist die Server-interne Linux-Firewall aktiviert. Für die OpenScape Business Funktionalität müssen bestimmte Ports/Dienste freigegeben werden (damit z. B. die Telefone mit OpenScape Business S kommunizieren können). Dies geschieht automatisch, der Administrator kann jedoch einzelne Dienste sperren.

Portnummern

Portnummern können Werte zwischen 0 und 65535 annehmen und werden so den verschiedenen Anwendungen zugeordnet. Zwischen 0 und 1023 liegen die sogenannten 'Well Known Ports', welche von der IANA (Internet Assigned Numbers Authority) fest zugeordnet worden und allgemein bekannt sind. Eine Liste dieser Ports können Sie unter http://www.iana.org/assignments/port-numbers einsehen.

19.1.1.1 Portfreigabe

Stellt das System den Internetzugang (über den WAN-Port) her, so ist standard-mäßig nur die Kommunikation erlaubt, die von innen (aus dem Firmennetz oder vom Kommunikationssystem selbst) ins Internet führt und die dazugehörigen Antwortpakete. Anfragen, die initial aus dem Internet kommen, werden geblockt. Diese Sicherheitseinstellung kann durch die gezielte Portfreigabe umgangen werden, um z. B. einen Webserver im Netz zu betreiben.

HINWEIS: Wenn das Kommunikationssystem als Internet Router genutzt wird, muss Port 5060 geschlossen sein (Standardeins-

tellung). Bei Internettelefonie über ITSP öffnet das Kommunikationssystem die relevanten Ports und hält diese offen.

Auch wenn ein externer Router bzw. Firewall genutzt wird, muss Port 5060 geschlossen sein. Es liegt in der Verantwortung des Kommunikationssystems diesen Port (falls benötigt) zu öffnen.

19.1.1.2 Wie Sie die Portfreigabe konfigurieren

Mit dem Wizard **Firewall** können Sie Portfreigaben aktivieren, so dass das Kommunikationssystem oder der PC am LAN über den WAN-Port erreichbar sind. Portfreigaben bergen das Risiko des Zugriffs durch Unbefugte. Daher sollten nur die Ports freigegeben werden, die dringend erforderlich sind.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Sicherheit**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Firewall** zu starten. Es öffnet sich das Fenster **Portfreigabe**.

4) Aktivieren Sie in der Zeile der gewünschten Anwendung bzw. des gewünschten Dienstes das Kontrollkästchen **NAT-Regel aktiv**, für die Sie Ports freigeben möchten.

5) Geben Sie in den Feldern **Globaler Port**, **Lokale IP-Adresse** und **Lokaler Port** jeweils die Daten zur Freigabe ein.

6) Klicken sie für die Portfreigabe eines nicht eingetragenen Dienstes auf **Hinzufügen** und füllen Sie die Felder **Beschreibung**, **NAT-Regel aktiv**, **Globaler Port**, **Lokale IP-Adresse** und **Lokaler Port** aus.

7) Klicken Sie auf **OK & Weiter**.

8) Klicken Sie auf **Beenden**.

19.1.1.3 Port-Verwaltung

Die Port-Verwaltung ermöglicht es, einige der Ports, die das Kommunikationssystem selbst verwendet, zu verändern. Dadurch kann z. B. in einem Netzwerk die Kommunikation auf das Kundennetz abgestimmt werden, auch wenn die Ports bereits anderweitig verwendet werden.

Wenn an der Portverwaltung Änderungen vorgenommen werden, muss dies in der Regel an allen Komponenten (Telefone, Anlagen etc.) gleichzeitig geändert werden, damit die Funktionalität gewährleistet bleibt.

19.1.1.4 Wie Sie globale Port-Manager-Einstellungen ändern

Hier geben Sie die Portnummern für die einzelnen Funktionen ein.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **Port-Verwaltung**. Es öffnet sich die Registerkarte **Globale Port-Manager-Einstellungen ändern**.

4) Geben Sie unter **Port-Nummer** den Port für die jeweilige Funktion ein, bzw. lassen die Voreinstellung bestehen.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

19.1.2 NAT

NAT (Network Address Translation) ist ein Adressenumsetzungsverfahren, um eine IP-Adresse in einem Datenpaket durch eine andere zu ersetzen. In einem internen Netz nutzen die Clients private IP-Adressen. Da private IP-Adressen in einem öffentlichen Netz nicht weitergeleitet werden, ist es mit NAT möglich, die privaten IP-Adressen auf eine öffentliche IP-Adresse abzubilden. Somit haben die internen Clients Zugang zum öffentlichen Netz und die Struktur des internen Netzes mit den privaten IP-Adressen ist gegenüber dem öffentlichen Netz (z. B. Internet) unsichtbar (maskiert). NAT bzw. NAT-Regeln werden für die Portfreigabe benötigt.

Die Adressenumsetzung wird an dem Übergang zwischen einem internen und einem öffentlichen Netz durchgeführt. NAT kann auf einem Internet-Router, einem Server oder einem anderen spezialisierten Gerät laufen. So kann z. B. ein Internet-Router mit Hilfe von NAT das interne Netz mit dem Internet verbinden.

Das interne Netz tritt gegenüber dem Internet mit nur einer einzigen öffentlichen IP-Adresse auf, die dem Internet-Router vom Internet-Service-Provider (ISP) zugewiesen wird. Alle Zugriffe aus dem internen Netz heraus in das Internet werden über diese offizielle IP-Adresse mit verschiedenen Port-Nummern abgewickelt. Der Internet-Router ersetzt die privaten IP-Adressen durch die vom ISP zugewiesene offizielle IP-Adresse. Bei ankommenden Datenpaketen wird die offizielle IP-Adresse wieder durch die privaten IP-Adressen ersetzt. Für die Zuordnung sind die jeweiligen Portnummern entscheidend. Nur extra freigeschaltete private IP-Adressen sind direkt aus dem Internet zu erreichen.

NAT-Regeln

Mit Hilfe von NAT-Regeln kann festgelegt werden, ob private (lokale) IP-Adressen direkt aus dem Internet erreichbar sein sollen. Dazu können eigene NAT-Regeln

definiert oder die bereits vorgeleisteten Standard-NAT-Regeln für die Dienste FTP-Server, HTTP-Server usw. verwendet werden. Insgesamt sind 20 NAT-Regeln definierbar. Um eine NAT-Regel zu nutzen, müssen die lokalen Adressendaten des Client-PCs eingegeben werden, der diese Dienste für das Internet zur Verfügung stellen will und die NAT-Regel muss aktiviert werden. Mehrere NAT-Regeln können zusammen mit Hilfe eines Tabelleneditors konfiguriert werden. Nicht mehr benötigte NAT-Regeln können gelöscht werden.

Ports

Startende Server fordern beim Betriebssystem bestimmte Ports an, um Verbindungen annehmen zu können. Ein HTTP-Server den Port 80, ein FTP-Server der Port 21 usw. Clients fordern beim Betriebssystem normalerweise einen zufälligen Port an, um Verbindungen aufbauen zu können.

19.1.2.1 Wie Sie eine NAT-Regel konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Routing**.

3) Konfigurieren Sie die NAT-Regel:

- Wenn Sie eine neue NAT-Regel definieren wollen, klicken Sie im Menübaum auf **NAT** und anschließend auf die Registerkarte **NAT hinzufügen**.
- Wenn Sie eine vorhandene NAT-Regel ändern wollen, navigieren Sie im Menübaum **NAT** zur gewünschten NAT-Regel.

4) Geben Sie im Feld **Beschreibung** einen Namen für die NAT-Regel an. Bei einer Standard-NAT-Regel kann dieser Name nicht geändert werden.

5) Geben Sie im Feld **Lokale IP-Adresse** die IP-Adresse des Clients im internen Netz ein, der freigeschaltet werden soll.

6) Geben Sie im Feld **Lokaler Port** die Port-Nummer ein, die die Anwendung des internen Clients verwendet.

7) Geben Sie im Feld **Globaler Port** die Port-Nummer ein, die die Anwendung des externen Kommunikationspartners verwendet.

8) Wählen Sie in der Aufklappliste **Protokoll** das von der Anwendung verwendende Transportprotokoll (**TCP** oder **UDP**) aus. Bei einer Standard-NAT-Regel kann das Protokoll nicht geändert werden.

9) Wenn Sie die NAT-Regel anwenden möchten, aktivieren Sie das Optionsfeld **NAT-Regel aktiv**.

10) Klicken Sie auf **Übernehmen** und anschließend auf **OK**. Die aktivierte NAT-Regel wird unter dem Menüpunkt **NAT** mit einem grünen Symbol gekennzeichnet.

19.1.2.2 Wie Sie mehrere NAT-Regeln mit dem NAT-Tabelleneditor konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie in der Navigationsleiste auf **Telefonie > Routing**.

3) Klicken Sie im Menübaum auf **Routing**.

4) Klicken Sie im Menübaum auf **NAT** und anschließend auf die Registerkarte **NAT Tabelleneditor**.

5) Konfigurieren Sie die NAT-Regel:

- Wenn Sie eine neue NAT-Regel definieren wollen, füllen Sie die Felder der ersten Zeile wie unten beschrieben aus.
- Wenn Sie eine vorhandene NAT-Regel ändern wollen, klicken Sie in die gewünschten Felder der NAT-Regel und füllen Sie diese wie unten beschrieben aus.

6) Geben Sie in der Spalte **Lokale IP-Adresse** die IP-Adresse des Clients im internen Netz ein, der freigeschaltet werden soll.

7) Geben Sie in der Spalte **Lokaler Port** die Port-Nummer ein, die die Anwendung des internen Clients verwendet.

8) Geben Sie in der Spalte **Globaler Port** die Port-Nummer ein, die die Anwendung des externen Kommunikationspartners verwendet.

9) Wählen Sie in der Aufklappliste **Protokoll** das von der Anwendung verwendende Transportprotokoll (**TCP** oder **UDP**) aus. Bei einer Standard-NAT-Regel kann das Protokoll nicht geändert werden.

10) Um die NAT-Regel anzuwenden, setzen Sie in der Spalte **Aktiv** das Häkchen.

11) Geben Sie in der Spalte **Beschreibung** einen Namen für die NAT-Regel an. Bei einer Standard-NAT-Regel kann dieser Name nicht geändert werden.

12) Speichern Sie die NAT-Regel:

- Wenn Sie eine neue NAT-Regel konfiguriert haben, klicken Sie auf **Hinzufügen** und anschließend auf **OK**. Die neue NAT-Regel wird am Ende der Tabelle eingefügt.
- Wenn Sie eine vorhandene NAT-Regel geändert haben, gehen Sie zu Schritt 5.

13) Klicken Sie auf **Übernehmen**. Eine aktivierte NAT-Regel wird unter dem Menüpunkt **NAT** mit einem grünen Symbol gekennzeichnet.

19.1.2.3 Wie Sie eine NAT-Regel löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Telefonie > Routing**.

2) Klicken Sie im Navigationsbaum auf **Routing**.

3) Klicken Sie im Menübaum auf **NAT**.

4) Klicken Sie im Menübaum auf die zu löschende NAT-Regel und klicken Sie auf die Registerkarte **NAT löschen**. Vordefinierte Standard-NAT-Regeln können nicht gelöscht werden.

5) Bestätigen Sie den Warnhinweis mit **Löschen** und klicken Sie anschließend auf **OK**. Die NAT-Regel wird unter dem Menüpunkt **NAT** aus der Liste der NAT-Regeln gelöscht.

19.1.3 Application Firewall

Die Application Firewall dient der Beschränkung des Zugriffs auf bestimmte Dienste (Services), wie z. B. FTP oder LDAP. Sie ist im Auslieferungszustand ausgeschaltet und lässt sich nach Definition entsprechender Regeln aktivieren.

Folgende Dienste können bei OpenScape Business X durch die Application Firewall auf bestimmte IP Adressen oder IP-Adressbereiche beschränkt oder gesperrt werden:

Dienst	Ports
FTP	21, 40000 - 40040
ssh (im Default gesperrt)	22
LDAP	389
HTTPS	443
Postgres	5432
Manager E	7000
CSTA	7001 (FP), 7004 (FP), 8800 (CSP)
Observer	8808

Nur die gelisteten Dienste können über ein Auswahlmenü im Expertenmodus gesperrt werden.

Telefonleistungsmerkmale wie SIP, HFA usw. können nicht über die Application Firewall gesperrt werden.

Ein Dienst kann mehrmals ausgewählt werden, jeweils mit unterschiedlichen IP-Restriktionen.

HINWEIS: Das Ein-/Ausschalten bzw. Ändern von Filterparametern kann die Funktionalität der Baugruppe extrem einschränken, z. B. könnte die Administration über LAN nicht mehr möglich sein.

19.1.3.1 Wie Sie die Konfiguration der Application Firewall anzeigen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.

3) Navigieren Sie im Menübaum zu **Application Firewall**.

4) Klicken Sie auf die Registerkarte **Display Services** um die gesperrten Dienste anzuzeigen.

5) Im Feld **Regelname** wird Ihnen der Name der Regel angezeigt.

6) Unter **Regel aktiviert** sehen Sie am Häckchen ob eine Regel aktiviert ist oder nicht.

7) Im Feld **Untergrenze des Quell-IP-Adressbereichs** sehen Sie die untere Grenze der gesperrten IP-Adressen.

8) Im Feld **Obergrenze des Quell-IP-Adressbereichs** sehen Sie die obere Grenze der gesperrten IP-Adresse.

19.1.3.2 Wie Sie Dienste über die Application Firewall einschränken

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.

3) Navigieren Sie im Menübaum zu **Application Firewall**.

4) Klicken Sie auf die Registerkarte **Add Service** um einen IP-Adressbereich bzw. Dienst zu sperren.

5) Vergeben Sie unter **Regelname** einen Namen für diesen Dienst (diese Regel).

6) Unter **Adressbereich** legen Sie die **Untergrenze** und die **Obergrenze** der zulässigen Quell-IP-Adressen fest.

Es ist möglich den Zugriff komplett zu sperren durch die Eingabe von 127.0.0.1.

INFO: Aktivieren sie eine Regel erst nachdem sie sich überzeugt haben, dass die berechtigten IP-Adressen korrekt konfiguriert wurden!

7) Klicken Sie auf **Speichern**.

19.1.3.3 Wie Sie die Konfiguration der Application Firewall löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.

3) Navigieren Sie im Menübaum zu **Application Firewall**.

4) Klicken Sie auf die Registerkarte **Delete all Services** um alle Dienste zu löschen.

19.1.4 Diensteverwaltung (OpenScape Business S)

Die Linux-interne Firewall ist standardmäßig aktiviert, wodurch der Zugriff auf OpenScape Business S unterbunden ist. Das Kommunikationssystem stellt allerdings Dienste zur Verfügung (z. B. den Dienst Telefonie), für den offene Ports (Dienste oder Services) erforderlich sind. Nach der Installation von OpenScape Business S sind diese erforderlichen Ports/Dienste in der Firewall geöffnet. Falls Dienste wie z. B. SNMP nicht genutzt werden sollen, können sie in der Linux-Firewall gesperrt werden.

HINWEIS: Beachten Sie, dass das Sperren von Diensten, die von OpenScape Business S verwendet werden, zu Beeinträchtigungen und/oder zum Ausfall der Funktionalität des Kommunikationssystems führen können.

19.1.4.1 Wie Sie Dienste hinzufügen oder sperren

Schritt für Schritt

1) Klicken Sie in der Taskleiste auf **Computer**.

2) Klicken Sie im Menübaum auf **System > YaST**.

3) Geben Sie das Passwort für den Benutzer root ein und klicken Sie auf **Continue**.

4) Klicken Sie im Menübaum auf **Security and Users**.

5) Klicken Sie im Bereich **Security and Users** auf **Firewall**.

6) Klicken Sie im Menübaum des Fensters **Firewall Configuration: Start-UP** auf **Allowed Services**.

7) Wählen Sie im Feld **Allowed Services for Selectet Zone** den Bereich aus, für den Sie Dienste ändern wollen (**External Zone**, **Demilitarized Zone**, **Internal Zone**).

8) Wählen Sie im Feld **Service to allow** die Dienste aus, die Sie gezielt freigeben (hinzufügen) möchten und klicken Sie auf **Add**. Im Pull-Down-Menü werden alle derzeit erlaubten Dienste aufgelistet.

9) Wählen Sie im Feld **Allowed Service** die Dienste aus, die Sie sperren möchten und klicken Sie auf **Delete**.

10) Aktivieren Sie ggf. das Kontrollkästchen **Protect Firewall from Internal Zone**.

11) Klicken Sie auf **Advanced** um ggf. Ports oder numerische Protokolle zur Firewall hinzuzufügen (**TCP Ports**, **UDP Ports**, **RPC Ports** und **IP Protocols**). Klicken Sie anschließend auf OK.

12) Klicken Sie auf **Next.** Die gemachten Einstellungen für die Firewall werden Ihnen angezeigt. Bei Bedarf können Sie über **Show Details** weitere Informationen einsehen.

13) Klicken Sie auf **Finish**.

19.2 Signaling and Payload Encryption SPE

SPE dient der Sicherheit bei der Übertragung von Signalisierungs- und Nutzdaten zwischen IP-Systemtelefonen und dem Kommunikationssystem. Dem Leistungsmerkmal liegt ein asymmetrisches Verschlüsselungsverfahren zugrunde, bei dem öffentliche und private Schlüssel verwendet werden.

Verschlüsselung der Signalisierungs- und Nutzdaten:

- Signaling Encryption: Die Signalübertragung zwischen Gateway und Clients wird mit einem 128-Bit-Schlüssel verschlüsselt. Für die Übertragung wird das TLS Protokoll mit AES-Verschlüsselung genutzt.
- Payload Encryption: Die Nutzdaten, auch Sprachdaten oder Payload genannt, werden mittels Secure Real-time Transport Protocol (SRTP)

übertragen. Sie werden mit einem 128-Bit-Schlüssel (AES) verschlüsselt. SRTP wird ebenfalls für die IP-Vernetzung verwendet. Das Verfahren zum Austauschen der Schlüssel für SRTP heißt Multimedia Internet KEYing oder kurz, MIKEY.

Für SPE muss gewährleistet werden, dass sich die einzelnen Systemtelefone und die beteiligten Kommunikationssysteme eindeutig identifizieren. Dies wird durch Zertifikate erreicht, die auch die öffentlichen Schlüssen bereitstellen.

Die Schlüssel bzw. Zertifikate werden durch den integrierten DLI-Server verteilt (können aber auch manuell verteilt werden).

INFO: WL2- und SIP-Telefone können nicht in Verbindung mit SPE genutzt werden.

Eine verschlüsselte Verbindung besteht nur in einer direkten Verbindung zweier Systemtelefone oder für Konferenzen.

SRTCP Verschlüsselung

SRTCP (Secure Real-Time Transport Control Protocol) ist eine Erweiterung des SRTP-Protokolls und realisiert die Sicherheit von Steuerungsdaten. Die Erweiterung besteht aus drei zusätzlichen Feldern: Einem SRTCP-Index, einem Encryption-Flag und einem Authentifizierungs-Tag.

SPE Konformität

Family / Protocol / Interface	Signalling Encryption							Payload Encryption				
	HFA Subscriber	SIP Subscriber	TDM Subscriber	Analog Subscriber	SIP-Q Trunking	ISDN CO	FAX (T38, G711)	HFA Subscriber2	SIP Subscriber2	TDM Subscriber2	Analog Subscriber2	IP-Q Trunking (GW)
OpenScape Office MX/LX												
HFA	s	nv	t	t	s	t	t	y	n	y	y	y
SIP-UA	t*	t*	nv	nv	t*	nv	nv	n	n	n	n	n
SIP-Trunking/ITSP	t*	nv	nv	nv	t*	nv	nv	n	n	n	n	n
SIP-Q Homogenous	s	t*	t	t	s	t	t*	y	n	y	y	y
Media Server / Conference	t	nv	nv	nv	t	nv	nv	n	n	n	n	n
Openscape Business X3/X5/X8												
HFA	s	nv	t	t	s	t	t	y	n	y	y	y
SIP-UA	t*	t*	nv	nv	t*	nv	nv	n	n	n	n	n
SIP-Trunking/ITSP	t*	nv	nv	nv	t*	nv	nv	n	n	n	n	n
SIP-Q Homogenous	s	t*	t	t	s	t	t*	y	n	y	y	y
SIP-Q Heterogenous - H4k	s	t*	t	t	s	t	t*	y	n	y	y	y
SIP-Q Heterogenous - OSV	s	t*	t	t	s	t	t*	y	n	y	y	y
Media Server / Conference	t	nv	nv	nv	t	nv	nv	n	n	n	n	n
MEB / VSL	t	nv	nv	nv	t	nv	nv	n	n	n	n	n

Legende:

nv	Keine VoIP Sicherheit
t	Standart: TLS auf der VoIP Seite; keine End-to-end Secure Payload
s	Signaling and Payload Encryption
*	Keine End-to-end Signaling Encryption (TLS)
*	
	Payload Encryption
y	Secure Payload (SRTP)
n	Non-Secure Payload (RTP)

19.2.1 Wie Sie SPE Unterstützung aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **System > System Flags**.

4) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie Signaling and Payload Encryption einschalten möchten, aktivieren Sie das Kontrollkästchen **SPE Unterstützung**.
- Wenn Sie Signaling and Payload Encryption ausschalten möchten, deaktivieren Sie das Kontrollkästchen **SPE Unterstützung**.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

19.2.2 Wie Sie SPE-Sicherheitseinstellungen ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Sicherheit > Signaling and Payload Encryption (SPE)**.

3) Wählen Sie in der Registerkarte **SPE Sicherheitseinstellungen ändern** unter **Minimale Länge des RSA Schlüssels** die minimale Schlüssellänge des Sicherheitsprotokolls aus (512, 1024 oder 2048).

4) Markieren Sie den Eintrag **Zertifikatsüberprüfung mit CRL-Überwachung**, wenn Sie einen Abgleich mit den CRL-Listen (Zertifikatswiderruflisten) wünschen.

5) Geben Sie unter **Maximales Interval für Schlüssel-Neuverhandlung (Stunden)** die Zeit (in Stunden) ein, nach der die Schlüsselpaare neu vergeben werden.

6) Markieren Sie **Subjectname überprüfen**, wenn Sie mit Subjektnamen verschlüsseln und diese bei jeder Verbindung überprüfen wollen.

7) Markieren Sie **Salt Key Verfahren verwenden**, wenn Sie mit Salt Keys verschlüsseln wollen.

8) Markieren Sie **SRTP Authentifizierung notwendig**, wenn Sie die Authentifizierung über das SRTP-Protokoll machen wollen.

9) Markieren Sie **SRTCP Verschlüsselung notwendig**, wenn Sie eine Verschlüsselung über das SRTCP-Protokoll machen.

10) Die **Länge des SRTP/SRTCP Authentifizierungs-Tag** ist vorgegeben.

11) Klicken Sie auf **Übernehmen**.

19.2.3 Wie Sie ein SPE-Zertifikat und den privaten Schlüssel importieren (PKCS#12)

Wenn kein kundenspezifisches Zertifikat zur Verfügung steht, kann über SSL > Zertifikatsgenerierung ein selbst signiertes CA-Zertifikat generiert werden und damit ein CA-signiertes Server Zertifikat (PKCS#12) erzeugt und abgespeichert werden. Dieses wird dann für SPE importiert.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Sicherheit > Signaling and Payload Encryption (SPE)**.

3) Navigieren Sie im Menübaum zu **SPE-Zertifikat**.

4) Geben Sie unter **SPE Zertifikat und privaten Schlüssel importieren (PKCS#12)** im Feld **Entschlüsselungskennwort** das beim Generieren der Datei entstandene Kennwort zur Entschlüsselung ein.

5) Geben Sie unter **Datei mit Zertifikat und privatem Schlüssel (PEM- oder PKCS#12-Format)** die Zertifikatsdatei ein bzw. wählen Sie diese durch **Durchsuchen** der Verzeichnisse.

> ***INFO:*** Wenn Sie bei aktiviertem SPE das erste Mal ein Zertifikat installieren wird anschließend automatisch ein Reset durchgeführt!

6) Klicken Sie auf **Fingerabdruck des Zertifikats anzeigen**, wenn Sie die Integrität überprüfen wollen.

19.2.4 Wie Sie das SPE CA-Zertifikat importieren

Dieser Schritt ist nicht erforderlich bei Verwendung von Zertifikaten die unter **SSL Zertifikatsgenerierung** selbst erzeugt worden sind.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Sicherheit > Signaling and Payload Encryption (SPE)**.
3) Navigieren Sie im Menübaum zu **SPE CA-Zertifikate**.
4) Geben Sie im Fenster **Verrtrauenswürdiges CA-Zertifikat (X.509 Datei) für SPE importieren** unter **Datei mit Zertifikat (PEM oder Binär-Format)** den Dateinamen der Zertifikatsdatei ein bzw. wählen Sie unter **Durchsuchen** die Datei aus.
5) Markieren Sie unter **CRL Distribution Point (CDP) Protokoll** das Protokoll für die CRL-Listen (Zertifikatswiderrufslisten) ein (**LDAP** oder **HTTP**).
6) Geben Sie unter **CDP (ohne z. B. ldap://)** den gewünschten Server ein.
7) Klicken Sie auf **Fingerabdruck des Zertifikats anzeigen**.

19.2.5 Wie Sie SPE für einen Teilnehmer aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Navigieren Sie im Menübaum unter **Teilnehmer > Teilnehmer > IP-Clients** zum gewünschten Teilnehmer (System-Client)
3) Navigieren Sie im Fenster **Teilnehmer** unter der Registerkarte **Teilnehmer-Parameter ändern** zum Eintrag **Payload Security**.
4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie die Funktion aktivieren möchten, wählen Sie unter **Payload Security** den Eintrag **Ein**.
   - Wenn Sie die Funktion deaktivieren möchten, wählen sie unter **Payload Security** den Eintrag **Aus**.
5) Klicken Sie auf **Übernehmen**.

19.3 Virtual Private Network VPN

Ein VPN (Virtual Private Network) ist ein Netz, das zum Transport privater Daten ein öffentliches Netz (z. B. das Internet) nutzt. Es ermöglicht somit eine sichere Übertragung über ein unsicheres Netzwerk. Die Übertragung von Daten geschieht dabei verschlüsselt.

VPN bietet:

- Sichere Verbindung über ein ungeschütztes Medium (Internet)

- Schutz vertraulicher Daten vor Manipulation
- Sichere Integration von externen Partnern (Teleworker) ins Firmennetz
- Zugriff auf Unternehmensinformationen für den Außendienst

Übersicht VPN

Um eine sichere Kommunikation zu gewährleisten, wird ein Tunnel zwischen den Kommunikationspartnern aufgebaut. Bei diesem Tunnelaufbau findet eine Authentifizierung und Autorisierung statt. Nach erfolgreichem Tunnelaufbau werden die eigentlichen Daten verschlüsselt übertragen.

Ein VPN kann zwischen (mindestens) zwei Geräten bzw. Netzen (Tunnelendpunkten) aufgebaut werden.

Es gibt 2 Vernetzungsarten:

- Site-to-Site-VPN
  Hierbei findet die Verschlüsselung zwischen zwei VPN-Gateways statt; innerhalb des LANs werden die Daten unverschlüsselt übertragen.
- End-to-Site-VPN
  Remote Access VPN (Fernzugriff von mobilen Mitarbeitern)

Systemspezifische Informationen

Die Administration der VPN-Parameter erfolgt über den Wizard **VPN**.

Beachten Sie, dass die Verbindung zum Kommunikationssystem über eine gesicherte Verbindung mit SSL verlaufen muss. Diese wird über OpenSwan und OpenSSL realisiert.

Abhängigkeiten

Thema	Abhängigkeit
DynDNS	Die VPN-Endpunkte müssen über einen Domain Namen oder eine feste IP-Adresse erreichbar sein. Ist dies nicht der Fall, kann DynDNS genutzt werden.
DynDNS	Wenn sich eine IP-Adresse bei VPN ändert, aktualisiert das Kommunikationssystem die auf den Hostnamen bezogenen Daten (IP-Adresse) im DynDNS.
DNS	Jeder VPN-Partner kann den Hostnamen/die IP-Adresse über das Standard-DNS-Protokoll auflösen. Sämtliche DNS-Namen (z. B. Hostname) müssen vollqualifizierte Domänennamen (FQDN) sein. Während der Aktualisierung der IP-Adresse über DNS sind keine Verbindungen über IPSec-Tunnels möglich.

19.3.1 Anforderungen für VPN

Um die Qualität der Sprach- und Datenübertragung sicherzustellen, müssen die verwendeten Netze bestimmte Anforderungen erfüllen. Besonders im Hinblick

auf eine Verschlüsselung ist mehr Bandbreite als bei einer anderen Vernetzung einzuplanen.

Für die folgenden Beispiele in den Tabellen wurde als Verschlüsselungsmodus "ESP Tunnel Modus mit Authentication" zugrunde gelegt. Dieser Modus bietet die höchste Sicherheit bei Site-to-Site VPNs.

Struktur eines verschlüsselten Sprachpaketes:

Protokoll	Bytes	
ESP Trailer	12	
ESP Padding	variiert (y)	verschlüsselt
ESP Padding Header	2	verschlüsselt
Voice Payload	variiert (x)	verschlüsselt
RTP	12	verschlüsselt
UDP	8	verschlüsselt
IP (original)	20	verschlüsselt
ESP-Header	8 + iv	
IP (Tunnel)	20	
802.1Q VLAN Tagging	4	
MAC (incl. Preamble, FCS)	26	
Summe	**112 + iv + x + y**	

Länge des ESP-Headers

Die Länge der ESP-Headers hängt vom verwendeten Verschlüsselungs-Algorithmus ab.

Erforderlich bei Cipher Block Chaining (Blockchiffre-Verkettung). Der ESP-Header enthält einen Initialisierungsvektor (IV). Die Länge des IV ist identisch mit der Länge des Chiffreblocks.

Padding

Padding ist erforderlich, da die Verschlüsselungs-Algorithmen auf Blockchiff-rierung beruhen. Dies bedeutet, dass der gesamte verschlüsselte Teil des Pakets (Original IP-/UDP-/RTP-Header + Sprach-Nutzlast + ESP-Header-Padding) einem ganzzahligen Vielfachen der Chiffreblocklänge entsprechen muss.

Blocklänge des Verschlüsselungs-Algorithmus:

Verschlüsselungs-Algorithmus	Blocklänge	Länge iv des Initialisierungs-Vektors
AES	16 Byte (128 Bit)	16 Byte (128 Bit)
3DES	8 Byte (64 Bit)	8 Byte (64 Bit)

Kalkulation der benötigten Padding-Bytes für Sprachpakete:

(42 + x + y) (Bytes) = N x (0 oder 16 (Bytes)) (N integer)

Bandbreiten-Kalkulation für den Verschlüsselungs-Algorithmus AES:

Codec	Paketierungs- Parameter	Rahmengröße (ms)	Payload (Bytes)	Padding (Bytes)	Ethernet Paketlänge (Bytes)	Payload/ Packet overhead ration	Ethernet Load (inkl.) Kopf (kBit/s)
G.711	20	20	160	6	294	75%	117,6
G.711	30	30	240	6	372	50%	99,2
G.711	40	40	320	6	454	38%	90,8
G.711	60	60	480	6	614	25%	81,9
G.729A	1	20	20	2	150	600%	60,0
G.729A	2	40	40	6	182	300%	36,4
G.729A	3	60	60	2	198	200%	26,4

Bandbreiten-Kalkulation für den Verschlüsselungs-Algorithmus DES / 3DES:

Codec	Paketierungs- Parameter	Rahmengröße (ms)	Payload (Bytes)	Padding (Bytes)	Ethernet Paketlänge (Bytes)	Payload/ Packet overhead ration	Ethernet Load (inkl.) Kopf (kBit/s)
G.711	20	20	160	6	286	75%	114,4
G.711	30	30	240	6	366	50%	97,6
G.711	40	40	320	6	446	38%	89,2
G.711	60	60	480	6	606	25%	80,8
G.729A	1	20	20	2	142	600%	56,8
G.729A	2	40	40	14	166	300%	33,2
G.729A	3	60	60	10	182	200%	24,3

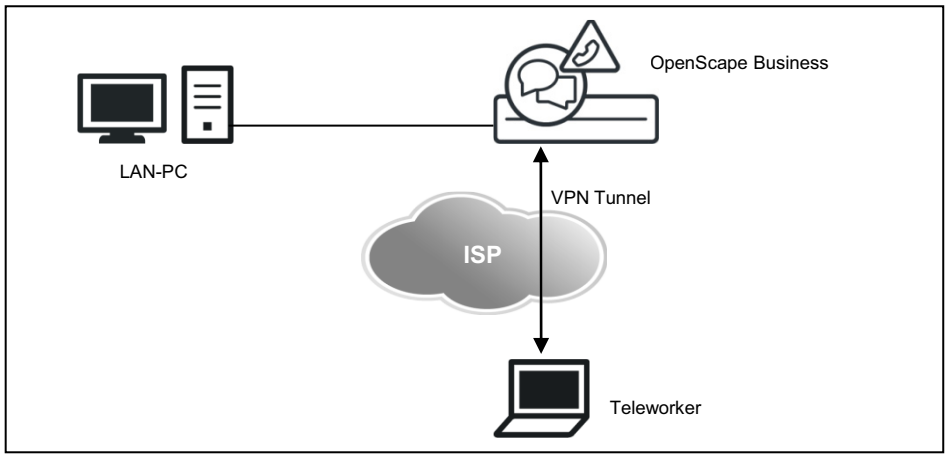
Bandbreite für Fax T.38

Verschlüsselungs-Algorithmus	Rahmengröße (ms)	Payload y (Bytes)	Padding x (Bytes)	Ethernet Paketlänge (Bytes)	Payload- Paket (Overhead in Prozent)	Ethernet Load (inkl.) Kopf (kBit/s)
DES / 3DES	30	169	1	278	64%	74,1
AES	30	169	9	294	74%	78.3

19.3.2 Anbindung von Teleworkern über VPN

Durch eine gesicherte Verbindung über VPN können Teleworker an das Kommunikationssystem angeschlossen werden.

Stand-alone-System mit Anbindung von Teleworkern über VPN



Das Kommunikationssystem verfügt über eine intergrierte VPN-Funktionalität (Konfiguration über Wizard). Bis zu 10 Teleworker können über VPN pro Kommunikationssystem gleichzeitig aktiv sein.

Folgende VPN-Clients sind für OpenScape Business freigegeben:

- NCP VPN Client
- Shrew Soft VPN Client
- iOS VPN Client
- Mac OS-X VPN Client

Export der Teleworker-Daten

Die Teleworker-Daten können als ZIP-Datei (unverschlüsselt) exportiert werden. In der ZIP-Datei befindet sich für jeden unterstützten VPN Client eine eigene Text-Datei mit den Teleworker-Daten - für den NCP VPN Client in Form einer `.ini`-Datei, für den Shrew Soft VPN Client in Form einer `.vpn`-Datei und für den OS-X VPN Client in Form einer `.networkConnect`-Datei. Diese Text-Dateien können am VPN-Client importiert werden.

> ***INFO:*** Evtl. vorkommende Umlaute oder Akzente werden in den Text-Dateien mit den Teleworker-Daten nicht behandelt. Leerzeichen werden durch Unterstriche ersetzt.

Statusanzeige der VPN-Verbindungen

Eine Statusanzeige aller VPN-Verbindungen finden Sie im Wizard **VPN**. Eine detailliertere Übersicht aller VPN-Verbindungen finden Sie im **Service-Center** unter **Diagnose > Status > VPN Status**.

VPN bei OpenScape Business S

Bei OpenScape Business S wird VPN über einen externen Router terminiert. Die Beschreibung von externen Applikationen ist nicht Bestandteil dieser Anleitung.

19.3.2.1 Wie Sie die Anbindung von Teleworkern über VPN konfigurieren

Mit dem Wizard **VPN** können Sie über VPN (Virtual Private Network) Teleworkern (VPN-Partnern) den Zugriff auf das interne LAN ermöglichen und Kommunikationssysteme per VPN verbinden. Hat das Kommunikationssystem keine feste externe IP-Adresse (öffentliche IP-Adresse, globale IP-Adresse), muss ein DynDNS-Service z. B. auf www.dyndns.org eingerichtet werden.

Voraussetzungen

- Der Internet-Zugang über die WAN-Schnittstelle ist konfiguriert.
- Hat die WAN-Schnittstelle keine feste (öffentliche) IP-Adresse, muss DynDNS konfiguriert sein. Für einen erfolgreichen DynDNS-Test wird eine Verbindung zum Internet benötigt.
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Netzwerk / Internet**.

3) Klicken Sie auf **Bearbeiten,** um den Wizard **VPN-Konfiguration** zu starten. Standardeinstellung ist **VPN ist ausgeschaltet**.

4) Klicken Sie auf **VPN konfigurieren**.

5) Wenn Sie eine konfigurierte VPN-Verbindung bearbeiten wollen, klicken Sie bei der gewünschten VPN-Verbindung auf **Bearbeiten**.

6) Wenn Sie eine neue VPN-Verbindung erstellen wollen, klicken Sie auf **Hinzufügen**.

7) Vergeben Sie im Feld **System Name** einen Namen für die VPN-Verbindung (z. B. `node2mch.dyndns.org`).

8) Geben Sie ggf. einen **Kommentar** in das dafür vorgesehe Feld ein.

9) Aktivieren Sie das Kontrollkästchen **aktiviert** (standardmäßig vorbelegt).

10) Markieren Sie das Kontrollkästchen **Daten des eigenen Systems verwenden**.

11) Wählen Sie bei Bedarf den **Adresstyp** aus:

- Hat die WAN-Schnittstelle eine feste (öffentliche) IP-Adresse, wählen Sie in der Aufklappliste **Adresstyp** den Eintrag **IP-Adresse** aus und geben Sie unter **globale IP-Adresse / DNS Name (WAN)** die feste (öffentliche) IP-Adresse ein.
- Hat die WAN-Schnittstelle keine feste (öffentliche) IP-Adresse, wählen Sie in der Aufklappliste **Adresstyp** den Eintrag **DNS-Name** aus. Unter **globale IP-Adresse / DNS Name (WAN)** wird der für DynDNS bereits konfigurierte DNS-Namen des Kommunikationssystems angezeigt.

12) Ändern Sie nur bei Bedarf die **lokale IP-Adresse (LAN)**.

13) Ändern Sie nur bei Bedarf die **lokale Subnetzmaske (LAN)**.

14) Wenn Sie einen bereits eingerichteten Teleworker bearbeiten wollen, klicken Sie im Bereich **Teleworker** beim gewünschten Teleworker auf **Bearbeiten**.

15) Wenn Sie einen neuen Teleworker einrichten wollen, klicken Sie im Bereich **Teleworker** auf **Hinzufügen**.

16) Vergeben Sie im Feld **Name** einen Namen für die Konfiguration dieses Teleworkers.

17) Konfigurieren Sie den Typ des verwendeten VPN-Clients:

- Für reine IPSec-VPN Teleworker (NCP und Shrew Soft VPN Clients):

  Deaktivieren Sie das Kontrollkästchen **L2TP/IPSec**, wählen Sie als **Adresstyp** den Eintrag **IP-Adresse** aus und geben Sie im Feld **virtuelle IP-Adresse / DynDNS-Name** eine virtuelle IP-Adresse für den Teleworker ein, wenn der eingesetzte VPN-Client virtuelle IP-Adressen unterstützt (unabhängig davon, ob der Teleworker per DSL-Router oder DSL-Modem Verbindung ins Internet hat).

- Für L2TP/IPSec-VPN Teleworker (iOS und MAC OS-X VPN Clients):

  Aktivieren Sie das Kontrollkästchen **L2TP/IPSec** und vergeben Sie **Benutzername** und **Passwort** für den Teleworker.

18) Aktivieren Sie das Kontrollkästchen **aktiviert** (standardmäßig vorbelegt).

19) Klicken Sie auf **OK**. Das Fenster mit der Übersicht über die Teleworker wird wieder angezeigt. Sie können weitere Teleworker eingeben.

20) Wenn Sie alle Teleworker eingerichtet haben, klicken Sie auf **OK & Weiter**. Das Fenster **System auswählen** wird angezeigt.

21) Klicken Sie auf **OK & Weiter**. Es öffnet sich das Fenster **Sicherheitseinstellungen für Verbindungen**.

22) Vergeben Sie für die gerade konfigurierte VPN-Verbindung einen Schlüssel für die sichere VPN-Verbindung unter **PreShared Secret** und wiederholen Sie diesen Schlüssel unter **Wiederholen des PreShared Secret**. Der Schlüssel muss mindestens 20 Zeichen lang sein.

23) Geben Sie ggf. noch einen **Kommentar** ein.

24) Klicken Sie auf **OK**. Es erscheint das Fenster **VPN Statusinformationen**.

25) Klicken Sie auf **VPN einschalten**.

26) Nur wenn als Adresstyp DNS-Name ausgewählt wurde: Kontrollieren Sie die bereits konfigurierten Daten des DynDNS-Accounts und klicken Sie auf **Verbindung testen**. Die DNS-Zugangsdaten werden zum Service-Provider übermittelt. Dieser Vorgang dauert ca. 10 Sekunden. Ist der Test nicht erfolgreich, überprüfen Sie bitte Ihre Zugangsdaten. Klicken Sie nach erfolgreichem Test auf **OK**.

27) Klicken Sie auf **OK & Weiter**. Die Teleworker greifen nun auf die WAN-Schnittstelle des Kommunikationssystems zu.

28) Klicken Sie auf **Beenden**.

19.3.2.2 Wie Sie die Teleworker-Daten exportieren

Mit dem Wizard **VPN** können Sie die Teleworker-Daten exportieren.

Voraussetzungen

- Eine VPN-Verbindung ist konfiguriert.
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Netzwerk / Internet**.

3) Klicken Sie auf **Bearbeiten,** um den Wizard **VPN-Konfiguration** zu starten. Standardeinstellung ist **VPN ist ausgeschaltet**.

4) Klicken Sie auf **Export/Import**.

5) Klicken Sie im Bereich **Exportieren der Teleworker-Daten vom System** auf **Export**. Speichern Sie die ZIP-Datei an einem Ort Ihrer Wahl.

> ***INFO:*** In der ZIP-Datei befindet sich für jeden unterstützten VPN-Client eine eigene Datei mit den Teleworker-Daten. Die Teleworker-Daten sind nicht verschlüsselt! Bitte gehen Sie mit den Daten verantwortungsbewusst um.

6) Klicken Sie auf **OK & Weiter** und abschließend auf **Beenden**.

19.3.3 Vernetzung von Kommunikationssystemen über VPN

Mehrere OpenScape Business Kommunikationssysteme können über eine Site-to-Site-VPN-Vernetzung sicher miteinander vernetzt werden.

Vernetzung über VPN

Sie haben die Möglichkeit in einem Kommunikationssystem alle Daten für eine Vernetzung mehrerer Systeme zu konfigurieren, diese Topologie-Daten verschlüsselt zu exportieren und in alle anderen Systeme im Netzverbund zu importieren. Dadurch wird an allen Systemen im Netzverbund eine schnelle und konsistente Konfiguration möglich.

Die Unterscheidung zwischen dem eigenen und den fremden Systemen findet über die Erkennung des eigenen DynDNS-Namens oder (bei Verwendung von festen IP-Adressen) über die eigene Internet-Adresse statt.

- Exportieren der Topologie-Daten vom System
  - Alle Daten über den Aufbau des VPN-Netzwerks werden in einer verschlüsselten XML-Datei zusammengefasst und als ZIP-Datei zum Export in ein anderes System bereitgestellt.

- Import der Topologie-Daten ins System
  - Alle Daten über den Aufbau des VPN-Netzwerks können als ZIP-Datei (beinhaltet die verschlüsselte XML-Datei) importiert und für dieses System übernommen werden.

Der Schlüssel (Passwort) für den Export ist frei wählbar und muss einem anderen Administrator, der diese Einstellungen importieren möchte, mitgeteilt werden.

Statusanzeige der VPN-Verbindungen

Eine Statusanzeige aller VPN-Verbindungen finden Sie im Wizard **VPN**. Eine detailliertere Übersicht aller VPN-Verbindungen finden Sie im **Service-Center** unter **Diagnose > Status > VPN Status**.

19.3.3.1 Wie Sie die Vernetzung über VPN konfigurieren

Mit dem Wizard **VPN** können Sie an einem System alle Kommunikationssysteme der VPN-Vernetzung konfigurieren. Diese Topologie-Daten können Sie exportieren und an allen Systemen im VPN-Netzverbund importieren.

Voraussetzungen

- Der Internet-Zugang über die WAN-Schnittstelle ist konfiguriert.
- Hat die WAN-Schnittstelle keine feste (öffentliche) IP-Adresse, muss DynDNS konfiguriert sein. Für einen erfolgreichen DynDNS-Test wird eine Verbindung zum Internet benötigt.
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Netzwerk / Internet**.

3) Klicken Sie auf **Bearbeiten,** um den Wizard **VPN-Konfiguration** zu starten. Standardeinstellung ist **VPN ist ausgeschaltet**.

4) Klicken Sie auf **VPN konfigurieren**.

5) Klicken Sie auf **Hinzufügen**.

6) Vergeben Sie im Feld **System Name** einen Namen für das erste System des VPN-Netzverbunds (z. B. `node1mch.dyndns.org`).

7) Geben Sie ggf. einen **Kommentar** in das dafür vorgesehe Feld ein.

8) Aktivieren Sie das Kontrollkästchen **aktiviert** (standardmäßig vorbelegt).

9) Markieren Sie das Kontrollkästchen **Daten des eigenen Systems verwenden**. Die nachstehenden Felder werden mit den Daten des Systems vorbelegt.

10) Wählen Sie nur bei Bedarf den vorbelegten **Adresstyp** aus:

- Hat die WAN-Schnittstelle eine feste (öffentliche) IP-Adresse, wählen Sie in der Aufklappliste **Adresstyp** den Eintrag **IP-Adresse** aus und geben Sie unter **globale IP-Adresse / DNS Name (WAN)** die feste (öffentliche) IP-Adresse ein.
- Hat die WAN-Schnittstelle keine feste (öffentliche) IP-Adresse, wählen Sie in der Aufklappliste **Adresstyp** den Eintrag **DNS-Name** aus. Unter **globale IP-Adresse / DNS Name (WAN)** wird der für DynDNS bereits konfigurierte DNS-Namen des Kommunikationssystems angezeigt.

11) Ändern Sie nur bei Bedarf die vorbelegte **lokale IP-Adresse (LAN)**.

12) Ändern Sie nur bei Bedarf die vorbelegte **lokale Subnetzmaske (LAN)**.

13) Klicken Sie auf **OK & Weiter**. Das Fenster **System auswählen** wird angezeigt.

14) Klicken Sie erneut auf **Hinzufügen**.

15) Vergeben Sie im Feld **System Name** einen Namen für das zweite System des VPN-Netzverbunds (z. B. `node2mch.dyndns.org`).

16) Geben Sie ggf. einen **Kommentar** in das dafür vorgesehe Feld ein.

17) Aktivieren Sie das Kontrollkästchen **aktiviert** (standardmäßig vorbelegt).

18) Wählen Sie den **Adresstyp** des zweiten Systems aus:

- Hat die WAN-Schnittstelle eine feste (öffentliche) IP-Adresse, wählen Sie in der Aufklappliste **Adresstyp** den Eintrag **IP-Adresse** aus und geben Sie unter **globale IP-Adresse / DNS Name (WAN)** die feste (öffentliche) IP-Adresse ein.
- Hat die WAN-Schnittstelle keine feste (öffentliche) IP-Adresse, wählen Sie in der Aufklappliste **Adresstyp** den Eintrag **DNS-Name** aus. Unter **globale IP-Adresse / DNS Name (WAN)** wird der für DynDNS bereits konfigurierte DNS-Namen des Kommunikationssystems angezeigt.

19) Geben Sie die **lokale IP-Adresse (LAN)** des zweiten Systems ein.

20) Geben Sie die **lokale Subnetzmaske (LAN)** des zweiten Systems ein.

21) Klicken Sie auf **OK & Weiter**. Das Fenster **System auswählen** wird angezeigt.

22) Wiederholen Sie die Schritte 14 bis 21 für weitere Systeme im VPN-Netzverbund.

23) Klicken Sie auf abschließend **OK & Weiter**. Es öffnet sich das Fenster **Sicherheitseinstellungen für Verbindungen**.

24) Vergeben Sie für jede VPN-Verbindung von einem System zum anderen einen eigenen Schlüssel unter **PreShared Secret** und wiederholen Sie diesen Schlüssel unter **Wiederholen des PreShared Secret**. Der Schlüssel muss mindestens 20 Zeichen lang sein.

25) Geben Sie ggf. noch einen **Kommentar** für jede VPN-Verbindung ein.

26) Klicken Sie auf **OK**. Es erscheint das Fenster **VPN Statusinformationen**.

27) Klicken Sie auf **Export/Import** um die Topologie-Daten zu exportieren. Es erscheint das Fenster **Exportieren und Importieren von VPN Konfigurationsdaten**.

28) Vergeben Sie im Bereich **Exportieren der Topologie-Daten vom System** unter **Schlüssel** und **Schlüssel wiederholen** einen Schlüssel (mind. 7-stellig) für die Sicherung der Daten und klicken Sie auf **Export**. Speichern Sie die ZIP-Datei an einem Ort Ihrer Wahl.

29) Klicken Sie auf **OK & Weiter**.

30) Klicken Sie auf **VPN einschalten**.

31) Nur wenn als Adresstyp **DNS-Name** ausgewählt wurde: Kontrollieren Sie die bereits konfigurierten Daten des DynDNS-Accounts und klicken Sie auf **Verbindung testen**. Die DNS-Zugangsdaten werden zum Service-Provider übermittelt. Dieser Vorgang dauert ca. 10 Sekunden. Ist der Test nicht erfolgreich, überprüfen Sie bitte Ihre Zugangsdaten. Klicken Sie nach erfolgreichem Test auf **OK**.

32) Klicken Sie auf **OK & Weiter** und abschließend auf **Beenden**.

33) Klicken Sie im WBM des zweiten Systems in der Navigationsleiste auf **Einrichtung** und im Navigationsbaum auf **Wizards > Netzwerk / Internet**.

34) Klicken Sie auf **Bearbeiten,** um den Wizard **VPN-Konfiguration** zu starten. Standardeinstellung ist **VPN ist ausgeschaltet**.

35) Klicken Sie auf **Export/Import** um die Topologie-Daten zu importieren. Es erscheint das Fenster **Exportieren und Importieren von VPN Konfigurationsdaten**.

36) Klicken Sie auf **Importieren der Topologie-Daten ins System** um die Topologiedaten zu importieren.

37) Geben Sie den **Schlüssel** (Passwort) ein, den Sie beim Export der Daten am ersten System eingegeben haben.

38) Navigieren Sie zum Ablageort der ZIP-Datei. Klicken Sie anschließend auf **Import**.

39) Klicken Sie auf **OK & Weiter**. Sie sehen die konfigurierten Systeme.

40) Klicken Sie auf **VPN einschalten**.

41) Nur wenn als Adresstyp **DNS-Name** ausgewählt wurde: Kontrollieren Sie die bereits konfigurierten Daten des DynDNS-Accounts und klicken Sie auf **Verbindung testen**. Die DNS-Zugangsdaten werden zum Service-Provider übermittelt. Dieser Vorgang dauert ca. 10 Sekunden. Ist der Test nicht erfolgreich, überprüfen Sie bitte Ihre Zugangsdaten. Klicken Sie nach erfolgreichem Test auf **OK**.

42) Klicken Sie auf **OK & Weiter** und abschließend auf **Beenden**.

43) Wiederholen Sie die Schritte 33 bis 42 für die restlichen Systeme im VPN-Netzverbund.

19.3.3.2 Wie Sie Topologie-Daten einer VPN-Vernetzung exportieren und importieren

Mit dem Wizard **VPN** können Sie die Topologie-Daten der Vernetzung über VPN exportieren und importieren.

Voraussetzungen

- Eine VPN-Verbindung ist konfiguriert.
- Für einen Import der Topologie-Daten müssen Sie den beim Export vergebenen Schlüssel wissen.
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Netzwerk / Internet**.

3) Klicken Sie auf **Bearbeiten,** um den Wizard **VPN-Konfiguration** zu starten. Standardeinstellung ist **VPN ist ausgeschaltet**.

4) Klicken Sie auf **Export/Import**.

5) Wenn Sie die Topologie-Daten exportieren wollen, vergeben Sie im Bereich **Exportieren der Topologie-Daten vom System** unter **Schlüssel** und **Schlüssel wiederholen** einen Schlüssel (mind. 7-stellig) für die Sicherung der Daten und klicken Sie auf **Export**. Speichern Sie die ZIP-Datei an einem Ort Ihrer Wahl.

6) Wenn Sie die Topologie-Daten importieren wollen, geben Sie im Bereich **Importieren der Topologie-Daten zum System** unter **Schlüssel** den Schlüssel für die Entschlüsselung der Daten ein und navigieren Sie zum Ablageort der ZIP-Datei. Klicken Sie abschließend auf **Import**.

7) Klicken Sie auf **OK & Weiter** und abschließend auf **Beenden**.

19.3.4 VPN - Sicherheitsmechanismen

Die Verschlüsselung der Daten geschieht bei VPN über verschiedene Sicherheitsmechanismen wie IPSec-Tunnel, Security Associations und Authentifizierungsmethoden (Peer-to-Peer, Digitale Signaturen).

IPSec-Tunnel

IPSec dient zur Verschlüsselung von Daten und kann generell mit und ohne Tunnel eingesetzt werden. IPSec ist eine Möglichkeit VPN zu realisieren. Es ist dabei möglich, das gesamte IP-Paket inklusive IP-Header zu verschlüsseln: Dies geschieht im Tunnelmodus.

Tunnel müssen immer bei beiden VPN-Partnern eingerichtet werden.

Bei IPSec kann die automatische Schlüsselverwaltung Internet Key Exchange (IKE) eingesetzt werden. Dabei handelt es sich um einen Standard, der in IPSec integriert ist.

Security Associations SA

Eine Security Association SA ist eine Vereinbarung zwischen zwei kommunizierenden Einheiten in Rechnernetzen. Sie beschreibt, wie die beiden Parteien Sicherheitsdienste anwenden, um sicher miteinander kommunizieren zu können.

VPN-Verbindungen erfordern immer drei Security Associations SA, die in zwei Phasen ausgehandelt werden:

- Phase 1 - Herstellen der IKE-SA
  eine für die anfängliche gegenseitige Authentifizierung und für den Austausch der Session-Keys (IKE-SA)
- Phase 2 - Aushandeln der Payload-SAs
  jeweils eine pro Richtung der aufgebauten Verbindung für den Payload-Verkehr (Payload-SAs)

IKE-SA

Das IKE-Protokoll hat im Wesentlichen zwei verschiedene Aufgaben. Zunächst ist eine ausschließlich vom IKE-Protokoll genutzte SA herzustellen (IKE-SA). Anschließend wird die vorhandene IKE-SA zur sicheren Aushandlung aller weiteren für die Übertragung von Payload-Daten benötigten SAs (Payload-SA) genutzt. IKE operiert daher in zwei aufeinanderfolgenden Phasen:

Beim Verbindungsaufbau zwischen den VPN-Partnern müssen diverse Parameter ausgehandelt werden (z. B. wie oft ein Schlüssel neu generiert wird oder welches Verschlüsselungsverfahren verwendet wird). Diese Parameter werden in IKE-SAs abgelegt und verwaltet.

Payload-SA

Die IKE-Phase 2 dient dem Aushandeln aller Sicherheitsparameter für die Payload-SAs zwischen den VPN-Partnern.

Es müssen immer zwei SAs hergestellt werden, für Übertragung und Empfang.

Im Wesentlichen werden folgende Schritte ausgeführt:

- Aushandeln der Algorithmen für Verschlüsselung und Authentifizierung
- Aushandeln der angewendeten Sicherheitsprotokolle (ESP und AH)
- Aushandeln des Betriebsmodus der Sicherheitsprotokolle
- Aushandeln der SA-Lebensdauer
- Festlegen des Schlüsselmaterials

Authentifizierung

Bei VPN findet eine Peer-to-peer-Kommunikation statt. Die Authentifizierung von VPN-Partnern ist auf zwei Arten möglich:

- Pre-shared Keys
  Meist werden bei VPN auch vorher verteilte Schlüssel (Preshared Keys) verwendet. Dazu wird bei beiden VPN-Partnern je ein Schlüsselpaar konfigu-

riert. Von diesen Schlüsseln wird zur Authentifizierung ein sogenannter Hash-Wert gebildet, den der jeweilige Partner überprüft.

- Digitale Signaturen
  Jedem VPN-Partner ist ein Zertifikat zugeordnet. Für eine erfolgreiche Authentifizierung müssen die VPN-Partner an beiden Tunnelendpunkten die digitale Signatur des jeweils gegenüberliegenden Partners gegen eine vertrauenswürdige CA prüfen.

Systemspezifische Informationen

Die Administration für die VPN-Parameter erfolgt prinzipiell über den Wizard.

Beachten Sie, dass die Administratorverbindung über eine gesicherte Verbindung mit SSL verlaufen muss.

- Security Associations SA
  Das Kommunikationssystem unterstützt die Oakley-Gruppen 1, 2 und 5
- IPSec
  Das Kommunikationssystem verwendet den IPSec-Tunnelmodus mit ESP (Encapsulating Security Payload). Bei ESP handelt es sich um ein IPSec-Protokoll, durch das die Paketverschlüsselung, Paketintegrität sowie die Paketauthentizität sichergestellt wird
- Payload SA
  Das Kommunikationssystem unterstützt als Verschlüsselungsalgorithmen DES, 3DES und AES
  Von den bekannten Gruppen von MAC-Algorithmen (MAC=Message Authentication Code) zur Authentifizierung von Datenherkunft und Datenintegrität werden HMAC-SHA1, HMAC-SHA2 und HMAC-MD5.
- Empfohlene Betriebsmodi
  - IKE im "Main Mode" mit Perfect Forward Secrecy
  - Hash-Funktion mit SHA-2
  - Authentifizierung mit Zertifikaten (RSA)
  - Verschlüsselung mit AES (bis zu 256 Bit)
  - Unterstützung dynamischer öffentlicher IP-Adressen über virtuelle IP-Adressen oder mittels DynDNS-Aktualisierungsmechanismen für Teleworker-PC

19.3.5 VPN - Zertifikate

Ein Zertifikat bindet einen bestimmten öffentlichen Schlüssel an einen bestimmten VPN-Client; bei dem Client kann es sich sowohl um einen Client des Kommunikationssystems als auch um einen Teleworker handeln. Die eindeutige Kombination aus öffentlichem Schlüssel und VPN-Client ist die Grundlage des Authentifizierungsvorgangs.

Zertifikate und Zertifizierungsstelle

Zertifikate werden digital signiert und von einer so genannten Zertifizierungsstelle (CA Certification Authority) ausgestellt. IPSec akzeptiert ein Zertifikat, wenn es von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt ist.

In einer einfachen VPN-Umgebung ist die Festlegung einer einzelnen Zertifizierungsstelle unter Umständen schon ausreichend; diese CA fungiert als vertrauenswürdige Stamm-Zertifizierungsstelle für das gesamte VPN und identifiziert sich gegenüber allen VPN-Clients anhand ihres selbst signierten CA-Zertifikats.

Jeder VPN-Client benötigt ein von dieser CA ausgestelltes Zertifikat.

Zertifikate nach dem X.509-Standard (dem heute gängigsten Standard) enthalten folgende Hauptelemente:

- Informationen über die Identität des Zertifikatseigentümers
- den öffentlichen Schlüssel des Zertifikatseigentümers
- Informationen bezüglich der CA, die das Zertifikat signiert hat (eine Seriennummer, die Gültigkeitsdauer, Informationen über die Identität der CA sowie die digitale Signatur der CA)

Lightweight-CA

Für Umgebungen, in denen der Kunde nicht bereits eine PKI nutzt, hilft eine Lightweight-CA-Funktionalität bei der Zertifizierung. Eine Lightweight-CA bietet folgende Möglichkeiten:

- Erstellen öffentlicher/privater Schlüsselpaare
- Signieren und Ausstellen entsprechender Zertifikate
- Speichern von Schlüsselpaaren mit zugehörigen Zertifikaten in Dateien

Als PKI (Public-Key-Infrastruktur) bezeichnet man in der Kryptografie ein System, welches es ermöglicht, digitale Zertifikate auszustellen, zu verteilen und zu prüfen.

CRL Certificate Revocation Lists - Zertifikatswiderrufslisten

Eine kritische Situation entsteht, wenn ein Zertifikat bekannt geworden ist (oder der Verdacht darauf besteht) und dieses Zertifikat für die Peer-Authentifizierung nicht mehr vertrauenswürdig ist. In diesem Fall muss die Zertifizierungsstelle das Zertifikat widerrufen und sämtliche Peers müssen baldmöglichst über den Widerruf informiert werden. Der Versuch eines Remote-Peers, seine Identität anhand eines widerrufenen Zertifikats zu authentifizieren, wird abgewiesen.

Grundsätzlich ist eine CRL eine Aufstellung sämtlicher widerrufener Zertifikate. CRLs müssen immer von der CA erzeugt werden, von der die Zertifikate stammen.

Eine CRL enthält folgende Hauptelemente:

- Aufstellung der widerrufenen Zertifikate; die Identifizierung der Zertifikate erfolgt durch die Seriennummern
- Zeitpunkt der Veröffentlichung der nächsten aktualisierten CRL (Angabe der Gültigkeitsdauer der CRL)

- Informationen bezüglich der CA, die das Zertifikat erzeugt hat (Informationen über die Identität der CA sowie die digitale Signatur der CA)

Eine regelmäßige Aktualisierung und Verteilung der CRLs muss manuell durch den Administrator erfolgen.

Systemspezifische Informationen

Die Authentifizierung erfolgt aufgrund von Algorithmen zur Kryptografie mit öffentlichen Schlüsseln. Das Kommunikationssystem unterstützt RSA als Algorithmus zur Kryptografie mit öffentlichen Schlüsseln. Das Kommunikationssystem unterstützt nur Zertifikate, die dem X.509-Standard entsprechen.

Das Kommunikationssystem agiert bei der Authentifizierung immer als VPN-Client.

- Lightweight CA
  Das Kommunikationssystem bietet eine eingeschränkte CA-Funktionalität (Lightweight CA). Der Administrator stellt für ein System das Schlüsselmaterial bereit, indem er manuell über die SSL-gesicherte Administrationsverbindung private/öffentliche Schlüsselpaare und Zertifikate in alle beteiligten Kommunikationspartner importiert
- CRL
  Es werden CRLs (Certificate Revocation Lists - Zertifikatswiderrufslisten) zum Widerruf von Zertifikaten verwendet. Der Import der CRL zum Kommunikationssystem geschieht durch den Administrator über eine SSL-gesicherte Verbindung.

19.3.5.1 VPN - Wie Sie Lightweight-CA-Zertifikate generieren

Lightweight CA ist eine lizenzpflichtige Funktion zum Generieren und Verwalten von CA- und Peer-Zertifikaten.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.

3) Navigieren Sie im Menübaum zu **VPN > Lightweight CA**. Im Fenster **Zertifikat generieren** können Sie ein eigenes CA-Zertifikat generieren.

4) Vergeben Sie unter **Name des Zertifikats** einen Namen für das angeforderte Zertifikat.

5) Vergeben Sie unter **Seriennummer des Zertifikats** eine Seriennummer für das Zertifikat.

INFO: Eine vergebene Seriennummer darf nicht noch einmal für ein anderes Zertifikat verwendet werden, da die Seriennummer aller jemals erzeugten Zertifikate eindeutig sein muss.

6) Geben Sie unter **Signatur-Algorithmus-Typ** den gewünschten Algorithmus für das Zertifikat ein (md5RSA, sha1RSA, sha256RSA oder sha512RSA).

7) Geben Sie unter **Länge des öffentlichen Schlüssels** die Länge des öffentlichen Schlüssels ein (z. B. 1024, 1536 oder 2048).

8) Geben Sie unter **Beginn der Zertifikatsgültigkeit (GMT)** Datum und Uhrzeit für den Beginn der Gültigkeit ein. Das Datum wird als Greenwich Mean Time (GMT) interpretiert.

9) Geben Sie unter **Ende der Zertifikatsgültigkeit (GMT)** Datum und Uhrzeit für das Ende der Gültigkeit ein.

10) Geben Sie unter **Antragsteller** das **Land (C)**, die **Organisation (O)**, die **Organisationseinheit (OU)** und **Allgemeiner Name (CN)** ein.

11) Optional können Sie unter **Alternativer Antragsteller** einen anderen Antragsteller eingeben. Wenn Sie dies getan haben, müssen Sie auch ein Format (z. B. IP-Adresse oder DNS-Name) eingeben. Das Eingabefenster ist von der Auswahl des Formats abhängig.

12) Geben Sie im Feld **CRL-Verteilungspunkt** den Verteilungspunkt für die CRL-Listen ein (werden in einer Pull-Down-Menü angezeigt).

13) Klicken Sie auf **Zertifikat erzeugen**.

19.3.5.2 VPN - Zertifikatsverwaltung - Wie Sie ein Zertifikat anzeigen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.

3) Navigieren Sie im Menübaum zu **VPN > Zertifikatsverwaltung**. Es öffnet sich das Fenster **Zertifikat aus Datei anzeigen**.

4) Aktivieren Sie ggf. das Kontrollkästchen **PKCS#12-Format**.

5) Geben Sie das **Entschlüsselungskennwort** ein.

6) Geben Sie unter **Datei mit dem Zertifikat** die Zertifikatsdatei an oder wählen Sie sie über das Feld **Durchsuchen** aus.

7) Klicken Sie auf **Laden**.

19.3.5.3 VPN - Wie Sie ein Trusted CA-Zertifikat importieren (X.509)

X.509 ist ein Standard für Zertifikate. Dabei werden im Zertifikat auch der Name und die digitale Signatur des Zertifikatsausstellers gespeichert. X.509 ist Bestandteil des Verzeichnisdienstes X.500 für weltweite, verteilte und offene Systeme.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.
3) Navigieren Sie im Menübaum zu **VPN > Zertifikatsverwaltung > Trusted CA-Zertifikate > Konfigurierte Zertifikate**.
4) Vergeben Sie unter **Name des Zertifikats** einen Namen für das angeforderte Zertifikat.
5) Geben Sie unter **Datei mit dem Zertifikat** die Zertifikatsdatei an oder wählen Sie diese über das Feld **Durchsuchen** aus.
6) Bestätigen Sie und klicken Sie auf **Aktivieren der konfigurierten VPN Tabellen.**

19.3.5.4 VPN - Peer Zertifikate - Wie Sie eine Zertifikatsanforderung (CSR) generieren

Sie können ein CA-signiertes Peer-Zertifikat, das auf einem CA-Zertifikat basiert, erzeugen. Voraussetzung ist, dass mindestens ein CA-Zertifikat generiert wurde. Das erzeugte Zertifikat wird in einer PKCS#12-Datei gespeichert. PKCS#12-Dateien (PKCS#12 Personal Information Exchange Syntax Standard) speichern Zertifikate mit dem privaten Schlüssel. Eine PKCS#12-Datei enthält also die entscheidenden Daten für persönliche Ver- und Entschlüsselung.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.
3) Navigieren Sie im Menübaum zu **VPN > Zertifikatsverwaltung > Peer-Zertifikate**.
4) Geben Sie in der Registerkarte **Zertifikatsanforderung (CSR) generieren** die erforderlichen Daten ein.
5) Geben Sie den **Name der Zertifikatsanforderung** ein.

6) Geben Sie unter **Signatur-Algorithmus-Typ** den gewünschten Algorithmus ein (sha1RSA, md5RSA, sha256RSA oder sha512RSA).

7) Geben Sie unter **Länge des Schlüssels** die Schlüssellänge ein (1024, 1536 oder 2048).

8) Geben Sie unter **Antragsteller** alle Daten für **Land (C)**, **Organisation (O)**, **Organisationseinheit (OU)** und **Allgemeiner Name (CN)** ein.

9) Geben Sie unter **Alternativer Antragsteller** das **Format des DN-Namens**, ein ggf. **Anderes Format** oder einen **Alternativen Antragsteller** ein.

10) Speichern Sie die *.csr Datei, die von einem CA signiert werden soll..

19.3.5.5 VPN - Peer Zertifikate - Wie Sie ein Zertifikat (PKCS#12) generieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.

3) Navigieren Sie im Menübaum zu **VPN > Lightweight CA**.

4) Klicken Sie auf das CA-Zertifikat, anschließend auf **CA-signiertes Peer Zertifikat (PKCS#12) generieren**.

5) Geben Sie das **Verschlüsselungskennwort** ein.

6) Geben Sie eine Seriennummer Ihrer Wahl unter **Seriennummer des Zertifikats** ein.

7) Geben Sie unter **Länge des Schlüssels** die Schlüssellänge ein (1024, 1536 oder 2048).

8) Geben Sie das Datum und die Zeit für den Start der Gültigkeitsperiode unter **Beginn der Zertifikatsgültigkeit (GMT)** ein. Das spezifizierte Datum ist Greenwich Mean Time.

> ***INFO:*** Die Gültigkeitsdauer des Peer Zertifikats sollte sorgfältig auf die im Unternehmen geltende Sicherheitsrichtlinie angepasst werden. Kurz vor Ablauf der Gültigkeitsperiode muß das Zertifikat verlängert oder ggf. ein neues Zertifikat ausgestellt werden.

9) Geben Sie das Datum und die Zeit für das Ende der Gültigkeitsperiode unter **Ende der Zertifikatsgültigkeit (GMT)** ein.

10) Geben Sie unter **Antragsteller** alle Daten für **Land (C)**, **Organisation (O)**, **Organisationseinheit (OU)** und **Allgemeiner Name (CN)** ein.

11) Optional können Sie unter **Alternativer Antragsteller** einen anderen Antragsteller eingeben. Wenn Sie dies getan haben, müssen Sie auch ein Format

(z. B. IP-Adresse oder DNS-Name) eingeben. Das Eingabefenster ist von der Auswahl des Formats abhängig.

12) Geben Sie den **CRL Verteilungspunkt** ein (optional).

13) Klicken Sie auf **Zertifikat erzeugen**.

19.3.5.6 VPN - Wie Sie ein Peer Zertifikat importieren (PKCS#12)

PKCS#12-Dateien (Personal Information Exchange Syntax Standard) speichern Zertifikate mit dem privaten Schlüssel. Eine PKCS#12-Datei enthält somit die entscheidenden Daten für die persönliche Ver- und Entschlüsselung.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.

3) Navigieren Sie im Menübaum zu **VPN > Zertifikatsverwaltung > Peer-Zertifikate**.

4) Klicken Sie auf die Registerkarte **Peer-Zertifikat importieren (PKCS#12)**.

5) Vergeben Sie unter **Name des Zertifikats** einen Namen für das angeforderte Zertifikat.

6) Geben Sie unter **Entschlüsselungskennwort** Ihr persönliches Kennwort zur Entschlüsselung dieses Zertifikats ein.

7) Geben Sie unter **Datei mit dem Zertifikat** den Dateinamen ein bzw. suchen Sie die Datei über die Schaltfläche **Durchsuchen**.

8) Klicken Sie auf **Fingerabdruck des Zertifikats anzeigen**.

9) Klicken Sie auf **Zertifikat aus Datei importieren**.

19.3.6 VPN-Clients

Ein Teleworker kann mit Hilfe eines VPN-Tunnels über das Internet eine sichere VPN-Verbindung zum Firmennetz herstellen. Dazu benötigt er auf seinem Gerät (PC, Tablet-PC, Smartphone) einen VPN-Client. Alle zwischen dem VPN-Client, der Firmen-Firewall und dem VPN-Server des Kommunikationssystems übertragenen Daten sind verschlüsselt.

Folgende VPN-Clients werden unterstützt:

- **NCP VPN Client**
  NCP-Clients können in beliebigen VPN-Umgebungen mit IPSec eingesetzt werden. Das ist von Bedeutung, wenn von einem Remote-PC auf VPN-Gateways verschiedener Hersteller zugegriffen werden soll oder bereits ein

zentrales VPN-Gateway von einem Dritthersteller im Firmennetz installiert ist. Im Falle einer Filialen-Vernetzung kann das NCP Secure Enterprise Gateway mit anderen VPN Gateways auf der Basis von IPSec-Verbindungen kommunizieren.
Der NCP-Client ist kostenpflichtig, bietet aber eine grafische Benutzeroberfläche und eine Statusanzeige der Verbindung.

- **Shrew Soft VPN Client**
  Der Shrew Soft VPN Client ist ein kostenloser VPN-Client mit grafischer Oberfläche, der ab Version 2.1.5 auch die Hybrid-Authentifizierung unterstützt.
  Der Shrew Soft VPN Client beinhaltet unter anderem ISAKMP, Xauth- und RSA-Unterstützung, AES, Blowfish, 3DES-Verschlüsselungsprotokolle und zahlreiche weitere Features, die sonst nur in professionellen Lösungen zu finden sind.
- **iOS VPN Client**
  Das Betriebssystem iOS hat den L2TP/IPSec VPN-Client integriert.
  Die L2TP/IPSec VPN-Clients benutzen den IP-Adress-Bereich `10.254.253.x`. Werden IP-Adressen aus diesem Bereich im Kundennetz bereits verwendet, muss der IP-Adress-Bereich im WBM geändert werden über **Experten-Modus > Wartung > Applikat.-Diagnose > IPSec Test: IPSec Test Routines > Set IP Address for L2TP** (z. B. von `10.254.253.1` auf `10.254.252.1`).
- **Mac OS-X VPN Client**
  Das Betriebssystem MAC OS-X hat den Mac OS-X-VPN-Client integriert.

Systemspezifische Informationen

- Die Teleworker-Daten eines VPN Clients können als ZIP-Datei (unverschlüsselt) exportiert werden. In der Zip-Datei befindet sich für jeden unterstützten VPN Client eine eigene Text-Datei mit den Teleworker-Daten - für den NCP VPN Client in Form einer `.ini`-Datei, für den Shrew Soft VPN Client in Form einer `.vpn`-Datei und für den OS-X VPN Client in Form einer `.networkConnect`-Datei. Diese Text-Dateien können am VPN-Client importiert werden.
- LAN-Infrastruktur mit mehreren Subnetzen
  Wenn bei einer LAN-Infrastruktur mit mehreren Subnetzen VPN genutzt werden soll, ist es notwendig Regeln für diese Subnetze zu erstellen. Die Regeln können nicht über den Wizard, sondern müssen über den Experten-Modus konfiguriert werden.
- Tunnel-im-Tunnel
  Es ist nicht möglich einen zweiten VPN-Tunnel durch einen bereits existierenden VPN-Tunnel zu führen.

19.3.6.1 NCP VPN Client Einstellungen

Für eine VPN-Anbindung über den NCP VPN Client sind die nachfolgend genannten Einstellungen zu beachten, wenn die Konfiguration manuell erfolgen soll. Über das Kommunikationssystem ist es möglich, eine Text-Datei

`ncp_vpn.ini` mit den konfigurierten VPN-Client-Daten zu exportieren und am VPN-Client zu importieren. Somit sind diese Einstellungen bereits vorbelegt.

Grundeinstellungen

- Profil-Name
  frei wählbar, aussagekräftiger Name zu empfehlen
- Verbindungstyp
  VPN zu IPSec-Gegenstelle
- Verbindungsmedium
  Gemäß der benutzten Internetverbindung
  z. B. LAN (over IP) oder xDSL (PPPoE)

Netzeinwahl

Keine Konfiguration notwendig.

HTTP-Anmeldung

Keine Konfiguration notwendig.

Modem

Keine Konfiguration notwendig.

Line Management

- Verbindungsaufbau
  automatisch oder manuell
  Timeout = 0

  INFO: Damit wird die Verbindung nicht mehr bei Leerlauf getrennt!

- Voice over IP (VoIP) priorisieren
  Haken setzen
- EAP-Authentisierung
  keine Konfiguration notwendig
- HTTP-Authentisierung
  keine Konfiguration notwendig

IPSec-Einstellungen

- Gateway = IP-Adresse oder DNS-Name des Kommunikationssystems
  Unter dieser IP-Adresse oder DNS-Name ist das Kommunikationssystem über das Internet zu erreichen
  Bezeichnung im VPN-Wizard: **IP-Adresse/DynDNS-Name**
- IKE-Richtlinie = Automatischer Modus
- IPSec-Richtlinie = Automatischer Modus
- Exchange Mode = Main Mode

- PFS-Gruppe = DH-Group 2 (1024 Bit)
- Gültigkeit / Dauer
  - IKE-Richtlinie: 000:00:07:00 (7 Minuten)
  - IPSec-Richtlinie: 000:00:08:00 (8 Minuten)
- Editor
  keine Konfiguration notwendig

Erweiterte IPSec-Optionen

keine Konfiguration notwendig

Identität

- Typ = IP Address
  ID = IP-Adresse des Teleworker PCs (siehe auch IP-Adressen-Zuweisung)
  Pre-shared Key verwenden
  Haken setzen
  Shared Secret = Dies ist das Passwort für die VPN-Verbindung
  Bezeichnung im VPN-Wizard: **PreShared Secret**
- Extended Authentication (XAUTH)
  nicht verwendet, keine Konfiguration notwendig

IP-Adressen-Zuweisung

- IP-Adresse manuell vergeben
  IP-Adresse = IP-Adresse des Teleworker PCs
  Bezeichnung im VPN-Wizard: **virtuelle IP Adresse/DNS-Name**
- DNS / WINS
  Haken setzen
- DNS-Server = IP-Adresse des Kommunikationssystems
  Bezeichnung im VPN-Wizard: **lokale IP-Subnetzadresse (LAN)**

VPN-IP-Netze

Keine Konfiguration notwendig

Zertifikats-Überprüfung

keine Konfiguration notwendig

Link Firewall

- Stateful Inspection aktivieren:
  bei bestehender Verbindung
- Ausschließlich Kommunikation im Tunnel zulassen:
  Haken setzen

19.3.6.2 Wie Sie einen NCP VPN Client konfigurieren

Für die sichere VPN-Verbindung zum Kommunikationssystem muss am Teleworker-Gerät ein NCP VPN Client installiert und konfiguriert werden.

Voraussetzungen

- Der Administrator Ihres Kommunikationssystems hat Sie im WBM von OpenScape Business als Teleworker eingerichtet und Ihnen die Export-ZIP-Datei mit den Teleworker-Daten zur Verfügung gestellt.
- Der Administrator Ihres Kommunikationssystems hat Ihnen den PreShared Secret Schlüssel für die VPN-Verbindung mitgeteilt.
- Auf dem Teleworker-Gerät ist der NCP VPN Client (LANCOM Advanced VPN-Client) installiert. Die dazu notwendigen Informationen finden Sie in der Dokumentation des NCP VPN Clients.
- Das Teleworker-Gerät hat eine bestehende, aktive Verbindung ins Internet.

Schritt für Schritt

1) Extrahieren Sie die Dateien `ncp_readme.txt` und `ncp_vpn.ini` und legen Sie diese in einem lokalen Verzeichnis ab. Die Einträge in der Datei `ncp_vpn.ini` beziehen sich auf das Profil `HOOME`.

2) Importieren Sie das Profil `HOOME` in den NCP VPN Client.

3) Erweitern Sie das Profil `HOOME` um einen DNS-Server. Die Adresse des DNS-Servers ist die private IP-Adresse (LAN) Ihres Kommunikationssystems.

4) Starten Sie den NCP VPN Client

5) Markieren Sie das Profil `HOOME` und klicken Sie auf **Connect**.

19.3.6.3 Wie Sie einen Shrew Soft VPN Client konfigurieren

Für die sichere VPN-Verbindung zum Kommunikationssystem muss am Teleworker-Gerät ein Shrew Soft VPN Client installiert und konfiguriert werden.

Voraussetzungen

- Der Administrator Ihres Kommunikationssystems hat Sie im WBM von OpenScape Business als Teleworker eingerichtet und Ihnen die Export-ZIP-Datei mit den Teleworker-Daten zur Verfügung gestellt.
- Der Administrator Ihres Kommunikationssystems hat Ihnen den PreShared Secret Schlüssel für die VPN-Verbindung mitgeteilt.
- Auf dem Teleworker-Gerät ist der Shrew Soft VPN Client installiert. Ein Download des Shrew Soft VPN Clients finden Sie unter `http://www.shrew.net`.
- Das Teleworker-Gerät hat eine bestehende, aktive Internet-Verbindung.

Schritt für Schritt

1) Extrahieren Sie die Dateien `shrewsoft_readme.txt` und `shrewsoft_openswan.vpn` und legen Sie diese in einem lokalen Verzeichnis ab.
2) Starten Sie den **Shrew Soft VPN Client Access Manager** und konfigurieren Sie diesen. Sichern Sie die Eingaben.
3) Importieren Sie die Datei `shrewsoft_openswan.vpn` in den Shrew Soft Client.
4) Anschließend sehen Sie im **Shrew Soft Client VPN Access Manager** unter **Connect** die Verbindung.

19.3.6.4 Wie Sie einen iOS VPN Client konfigurieren

Für die sichere VPN-Verbindung zum Kommunikationssystem muss am Teleworker-Gerät eine L2TP-VPN-Verbindung konfiguriert werden.

Voraussetzungen

- Der Administrator Ihres Kommunikationssystems hat Sie im WBM von OpenScape Business als Teleworker eingerichtet und Ihnen Benutzername, Kennwort und PreShared Secret Schlüssel für die VPN-Verbindung mitgeteilt.
- Das Teleworker-Gerät hat eine bestehende, aktive Verbindung ins Internet.

Schritt für Schritt

1) Öffnen Sie am iOS-Teleworker-Gerät das Menü **Einstellungen > Allgemein > VPN**.
2) Fügen Sie mit **VPN hinzufügen** eine neue VPN-Verbindung hinzu.
3) Klicken Sie auf die Registerkarte **L2TP**.
4) Vergeben Sie im Feld **Beschreibung** einen Namen für diese VPN-Verbindung.
5) Geben Sie im Feld **Server** die öffentliche IP-Adresse oder den DNS-Namen des Kommunikationssystems ein.
6) Geben Sie im Feld **Account** den Teleworker-Benutzernamen ein.
7) Geben Sie im Feld **Kennwort** das Teleworker-Kennwort ein.
8) Geben Sie im Feld **Shared Secret** den Schlüssel (Preshared Secret) des VPN-Tunnels ein.
9) Aktivieren Sie den Schalter **Für alle Daten**.
10) Aktivieren Sie im Menü **Einstellungen** den Schalter **VPN**.

19.3.6.5 Wie Sie einen Mac OS-X VPN Client konfigurieren

Für die sichere VPN-Verbindung zum Kommunikationssystem muss am Teleworker-Gerät eine L2TP-VPN-Verbindung konfiguriert werden.

Voraussetzungen

- Der Administrator Ihres Kommunikationssystems hat Sie im WBM von OpenScape Business als Teleworker eingerichtet und Ihnen die Export-ZIP-Datei mit den Teleworker-Daten zur Verfügung gestellt.
- Der Administrator Ihres Kommunikationssystems hat Ihnen Benutzername, Kennwort und PreShared Secret Schlüssel für die VPN-Verbindung mitgeteilt.
- Das Teleworker-Gerät hat eine bestehende, aktive Verbindung ins Internet.

Schritt für Schritt

1) Extrahieren Sie die Datei `.networkConnect` und legen Sie diese in einem lokalen Verzeichnis ab.

2) Klicken Sie auf die Datei `.networkConnect` doppelt.

3) Klicken Sie auf **VPN (L2TP)**.

4) Wählen Sie im Feld **Konfiguration** die VPN-Verbindung aus.

5) Geben Sie im Feld **Serveradresse** die öffentliche IP-Adresse oder den DNS-Namen des Kommunikationssystems ein.

6) Geben Sie im Feld **Benutzername** den Teleworker-Benutzernamen ein.

7) Setzen Sie die Sicherheitseinstellungen:

a) Klicken Sie auf **Authentifizierungseinstellungen**.

b) Geben Sie im Feld **Kennwort** das Teleworker-Kennwort ein.

c) Geben Sie im Feld **Schlüssel ("Shared Secret")** den Schlüssel (Preshared Secret) des VPN-Tunnels ein.

d) Klicken Sie auf **OK**.

8) Klicken Sie auf **Weitere Optionen** und aktivieren Sie das Kontrollkästchen **Gesamten Verkehr über die VPN-Vebindung senden**. Klicken Sie abschließend auf **OK**.

9) Klicken Sie auf **Anwenden** und anschließend auf **Verbinden**. Bei erfolgreicher Verbindung zur OpenScape Business wird als Status **Verbunden** angezeigt.

19.3.7 VPN - Dienste

Über die Funktion Konfigurierte Dienste können Sie Dienste verwalten. Konfigurierte Dienste werden erst durch Aktivieren zu aktiven Diensten.

19.3.7.1 VPN - Aktive Dienste - Wie Sie alle IPsec-Dienste anzeigen

Sie können eine Liste aller aktiven IPsec-Dienste mit Detaildaten in Tabellenform ansehen.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.
3) Navigieren Sie im Menübaum zu **VPN > Dienste > Aktive Dienste**.
4) Unter der Registerkarte **IPsec-Dienste anzeigen** können Sie die Detaildaten für die aktiven IPsec-Dienste ansehen.

19.3.7.2 VPN - Aktive Dienste - Wie Sie einen speziellen IPsec-Dienst anzeigen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.
3) Navigieren Sie im Menübaum zu **VPN > Dienste > Aktive Dienste**.
4) Klicken Sie im Menübaum den speziellen Dienst an, zu dem Sie alle Informationen einsehen möchten (**Name des Dienstes**, **Quell-Port**, **Ziel-Port**, **IP-Protokoll**, **Zugehörige 'pass'-Regel**, **Zugehörige 'deny'-Regel**).

19.3.7.3 VPN - Konfigurierte Dienste - Wie Sie alle IPsec-Dienste anzeigen

Sie können eine Liste aller konfigurierten IPsec-Dienste mit Detaildaten in Tabellenform ansehen.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.
3) Navigieren Sie im Menübaum zu **VPN > Dienste > Konfigurierte Dienste**.

4) Unter der Registerkarte **IPsec-Dienste anzeigen** können Sie die Detaildaten für die konfigurierten IPsec-Dienste ansehen.

19.3.7.4 VPN - Konfigurierte Dienste - Wie Sie den IPsec-Dienst ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

> ***INFO:*** Vor dem Ändern bzw. Einschalten des IPsec-Dienstes sollte ein Backup durchgeführt werden. IPsec-Regeln verhalten sich wie Firewall-Einträge und können den Zugriff auf das System einschränken. Sollte es doch vorkommen, dass Sie IPsec aktivieren und keinen Zugriff mehr auf das System haben, können Sie das Kommunikationssystem mit **Reload** zurücksetzen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.

3) Navigieren Sie im Menübaum zu **VPN > Dienste > Konfigurierte Dienste**.

4) Klicken Sie im Menübaum den speziellen Dienst an, den Sie ändern möchten.

5) Ändern Sie den Namen des Dienstes unter **Name des Dienstes**.

6) Ändern Sie den Quell-Port unter **Quell-Port**.

7) Ändern Sie den Ziel-Port unter **Ziel-Port**.

8) Ändern Sie unter **IP-Protokoll** den Dienst (z. B. UDP).

9) Nach der gesamten VPN-Konfiguration wird die Änderung mit **Aktivieren der konfigurierten VPN Tabellen** übernommen

19.3.7.5 VPN - Konfigurierte Dienste - Wie Sie den IPsec-Dienst umbenennen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.

3) Navigieren Sie im Menübaum zu **VPN > Dienste > Konfigurierte Dienste**.

4) Klicken Sie im Menübaum den speziellen Dienst an, den Sie umbenennen möchten.

5) Ändern Sie unter **Name des Dienstes** den Namen des Dienstes.

6) Nach der gesamten VPN-Konfiguration wird die Änderung mit **Aktivieren der konfigurierten VPN Tabellen** übernommen

19.3.7.6 VPN - Konfigurierte Dienste - Wie Sie den IPsec-Dienst löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.

3) Navigieren Sie im Menübaum zu **VPN > Dienste > Konfigurierte Dienste**.

4) Klicken Sie im Menübaum den speziellen Dienst an, den Sie löschen möchten.

5) Nach der gesamten VPN-Konfiguration wird die Änderung mit **Aktivieren der konfigurierten VPN Tabellen** übernommen

19.3.8 VPN - Tunnel

Ein Tunnel bezeichnet einen Transport von verschlüsselten Datenpaketen zu einem fest definierten Endpunkt. Aktive Tunnel sind konfigurierte Tunnel nach einer Aktivierung der Konfiguration. Insgesamt lassen sich bis zu 256 Tunnel pro Gateway einrichten.

19.3.8.1 VPN - Aktive Tunnel - Wie Sie allgemeine Tunneldaten anzeigen

Sie können alle aktiven Tunneldaten in Tabellenform mit Detailinformationen ansehen.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.

3) Navigieren Sie im Menübaum zu **VPN > Tunnel > Aktive Tunnel**.

4) Unter der Registerkarte **Allgemeine Tunneldaten anzeigen** sehen Sie die Detailinformationen zu den jeweils aktiven Tunneln, wie

Name des Tunnels
Status im IP-Stack
Endpunktyp des lokalen Tunnels
Endpunktadresse des lokalen Tunnel
Endpunkttyp des Remote Tunnel
Endpunktadresse des Remote Tunnel
Vorgeschlagene Lebensdauer der Session-Keys
Vorgeschlagene Lebensdauer der Schlüsseltausch-Session
Zugehörige Regeln Zugehörige Senderegel
Zugehörige Regeln Zugehörige Empfangsregel

19.3.8.2 VPN - Aktive Tunnel - Wie Sie Regeln für alle Tunnel anzeigen

Sie können sich in einem Fenster die Regeln für alle aktiven Tunnel anzeigen.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.

3) Navigieren Sie im Menübaum zu **VPN > Tunnel > Aktive Tunnel**.

4) Unter der Registerkarte **Regeln für alle Tunnel anzeigen** sehen Sie die Detailinformationen zu den jeweils aktiven Tunneln, wie

Tunneldaten
Regeldaten
Quelladresse
Zieladresse
Dienstdaten

19.3.8.3 VPN - Konfigurierte Tunnel - Wie Sie allgemeine Tunneldaten anzeigen

Sie können alle Daten für konfigurierte Tunnel in Tabellenform mit Detailinformationen ansehen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.
3) Navigieren Sie im Menübaum zu **VPN > Tunnel > Konfigurierte Tunnel**.
4) Unter der Registerkarte **Allgemeine Tunneldaten anzeigen** sehen Sie die Detailinformationen zu den jeweils konfigurierten Tunneln, wie
   Name des Tunnels
   Endpunktyp des lokalen Tunnels
   Endpunktadresse des lokalen Tunnel
   Endpunkttyp des Remote Tunnel
   Endpunktadresse des Remote Tunnel
   Vorgeschlagene Lebensdauer der Session-Keys
   Vorgeschlagene Lebensdauer der Schlüsseltausch-Session
   Zugehörige Regeln Zugehörige Senderegel
   Zugehörige Regeln Zugehörige Empfangsregel

19.3.8.4 VPN - Konfigurierte Tunnel - Wie Sie Regeln für alle Tunnel anzeigen

Sie können sich in einem Fenster die Regeln für alle konfigurierten Tunnel anzeigen.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.
3) Navigieren Sie im Menübaum zu **VPN > Tunnel > Konfigurierte Tunnel**.
4) Unter der Registerkarte **Regeln für alle Tunnel anzeigen** sehen Sie die Detailinformationen zu den jeweils konfigurierten Tunneln, wie
   Tunneldaten
   Regeldaten
   Quelldaten
   Zieldaten
   Dienstdaten

19.3.8.5 VPN - Wie Sie einen konfigurierten Tunnel hinzufügen

Sie können einen neuen IPsec-Tunnel einrichten. Insgesamt lassen sich bis zu 256 Tunnel pro Gateway einrichten.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.

3) Navigieren Sie im Menübaum zu **VPN > Tunnel > Konfigurierte Tunnel**.

4) Unter der Registerkarte **Tunnel hinzufügen** erhalten Sie das Eingabefenster für den neuen Tunnel.

5) Markieren Sie **Tunneldaten**.

6) Geben Sie unter **Name des Tunnels** den gewünschten Namen für den neuen Tunnel ein.

7) Wählen Sie in der Aufklappliste **Endpunkttyp des lokalen Tunnel** den Typ der Endpunktadresse auf der Tunnel-Sendeseite aus (möglich ist die Angabe eines Host- oder DNS-Namens).

8) Geben Sie unter **Endpunktadresse des lokalen Tunnel** die Senderadresse in dem zum Endpunkttyp passenden Format ein.

9) Wählen Sie in der Aufklappliste **Endpunkttyp des Remote Tunnel** den Typ der Endpunktadresse auf der Tunnel-Empfängerseite aus (es wird die Angabe der IP-Adresse unterstützt).

10) Geben Sie unter **Endpunktadresse des Remote Tunnel** die Empfängeradresse in dem zum Endpunkttyp passenden Format ein. Wird die Adresse 0.0.0.0 eingestellt, so bedeutet dies, dass der Tunnelendpunkt unbekannt ist. In diesem Fall muss der Tunnelaufbau immer von der Gegenstelle erfolgen (z. B. Teleworker).

11) Geben Sie unter **Session-Key-Handhabung** das Verfahren für den Schlüsselaustausch ein (möglich ist: Automatisch, mit dem IKE-Protokoll).

12) Wählen Sie unter **Vorgeschlagene Verschlüsselungsalgorithmen** aus, welche Algorithmen verwendet werden dürfen (AES oder 3DES).

13) Wählen Sie unter **Vorgeschlagene Hash-Algorithmen** aus, welche Prüfalgorithmen verwendet werden dürfen (MD5, SHA1 oder SHA2). Die ausgewählten Algorithmen werden vom Initiator der IKE-Aushandlung angeboten.

14) Geben Sie unter **Vorgeschlagene Lebensdauer der Session-Keys** eine Gültigkeitsdauer für die Session Keys (Sitzungsschlüssel) ein, die verwendet werden. Nach Ablauf dieser Zeit werden keine Daten mehr innerhalb dieser Sitzung ausgetauscht. Als Ersatz für ungültig gewordene Session Keys werden automatisch neue Session Keys ausgehandelt.

15) Geben Sie unter **Vorgeschlagene Lebensdauer der Schlüsseltausch-Session** eine Gültigkeitsdauer ein. Nach Ablauf der Schlüsseltausch-Session werden automatisch neue Schlüssel durch IKE ausgehandelt.

16) Geben Sie unter **Vorgeschlagene Datenvolumen der Session-Keys** das maximale Datenvolumen für die Session Keys ein. Nach Überschreiten des

Datenvolumens wird automatisch ein neuer Session-Key mittels IKE ausgehandelt. Bei der Auswahl von **unbegrenzt** wird die Gültigkeit der Session Keys nicht durch die Datenmenge begrenzt.

17) Aktivieren Sie im oberen Teil des Fensters das Kontrollkästchen **Schlüsseltauschdaten**.

18) Geben Sie alle Schlüsseltauschdaten ein (**'Perfect Forward Secrecy' aktivieren und wählen Sie das Authentifizierungsverfahren für die VPN-Peers** (**Pre-Shared-Key** oder **Digitale Signaturen**) aus.

INFO: Wenn Sie als Authentifizierungsverfahren **Pre-Shared Keys** gewählt haben, so müssen Sie einen 20stelligen Pre-Shared Key eingeben (und diesen wiederholen).

INFO: Wenn Sie als Authentifizierungsverfahren **Digitale Signaturen** (von einem Lightweight CA) in einem VPN-Netzwerk mit mehreren Knoten nutzen, müssen Sie zusätzliche Schritte konfigurieren.

---

a) Erstellen Sie ein LWCA-Zertifikat an einem Knoten.

b) Exportieren Sie das Zertifikat (.crt) in eine Datei.

c) Erstellen und exportieren Sie eine Certificate Revocation List (.crl) in eine Datei.

d) Erstellen und exportieren Sie ein Peer-Zertifikat (.p12), das vom CA-Zertifikat signiert ist, für jeden Knoten.

e) Das CA-Zertifikat (.crt), die Certificate Revocation List (.crl) und die entsprechenden Peer-Zertifikate müssen in jeden Knoten importiert werden.

19) Geben Sie die **Vorgeschlagene Diffie-Hellmann-Gruppen** (DH-Gruppe 2, 5 oder 14) ein.

20) Nach der gesamten VPN-Konfiguration wird die Änderung mit **Aktivieren der konfigurierten VPN Tabellen** übernommen

19.3.9 VPN - Regeln

Regeln legen fest, was mit einem IP-Paket geschehen soll. Die Regelaktion *Pass* bedeutet, dass das IP-Paket weitertransportiert (durchgelassen) wird. Die Regelaktion *Deny* bedeutet, dass das IP-Paket nicht weitertransportiert (ignoriert) wird. Es kann jeweils ausgewählt werden, ob das IP-Paket einen (verschlüsselten) VPN-Tunnel benutzt oder nicht.

Das Kommunikationssystem kann 640 Regeln verwalten, davon sind 6 Regeln vorbelegt (Default-Regeln) und 634 frei zur Vergabe.

19.3.9.1 VPN - Aktive Regeln - Wie Sie Regeln anzeigen

Sie können sich alle aktiven Regeln anzeigen lassen.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.

3) Navigieren Sie im Menübaum zu **VPN > Regeln > Aktive Regeln**.

4) Klicken Sie auf die Registerkarte **Regeln anzeigen,** dann sehen Sie die Detailinformationen zu der aktiven Regeln, wie

Priorität
Dienst
Aktion für die Regel
Verschlüsselung erforderlich
Regel-Status
Status im IP-Stack
Quelladresse
Zieladresse)
Tunnel für die Verschlüsselung

19.3.9.2 VPN - Aktive Regeln - Wie Sie spezielle Regel anzeigen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.

3) Navigieren Sie im Menübaum zu **VPN > Regeln > Aktive Regeln**.

4) Klicken auf die gewünschte Regel im Menübaum. Das Fenster **Regel anzeigen** mit allen Detaildaten erscheint für diese Regel (**Priorität**, **Dienst**, **Aktion für die Regel**, **Verschlüsselung erforderlich**, **Regel-Status**, **Quell-adresse**, **Zieladresse**)

19.3.9.3 VPN - Konfigurierte Regeln - Wie Sie alle Regeln anzeigen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.

3) Navigieren Sie im Menübaum zu **VPN > Regeln > Konfigurierte Regeln**.

4) Klicken Sie auf die Registerkarte **Regeln anzeigen,** dann sehen Sie die Detailinformationen zu der aktiven Regeln, wie

Priorität
Dienst
Aktion für die Regel
Verschlüsselung erforderlich
Regel aktivieren
Quelladresse (Typ und IP-Adresse)
Zieladresse (Typ und IP-Adresse)

19.3.9.4 VPN - Konfigurierte Regeln - Wie Sie eine Regel hinzufügen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.

3) Navigieren Sie im Menübaum zu **VPN > Regeln > Konfigurierte Regeln > Regel hinzufügen**.

4) Nehmen Sie die Einstellungen für folgende Parameter vor:

Priorität

Dienst

Aktion für die Regel (PASS, PASS_INCOMING, PASS_OUTGOING, DENY)

Verschlüsselung erforderlich

Regelstatus

Quelladresse - Typ

Quelladresse - Adresse (unterste des Bereichs)

Quelladresse - Subnetzmaske (oberste Adr. des Bereichs)

Zieladresse - Typ

Zieladresse - Adresse (unterste des Bereichs)

Zieladresse - Subnetzmaske (oberste Adr. des Bereichs)

Tunnel auf der Empfangsseite

Tunnel auf der Sendeseite

5) Klicken Sie auf **Übernehmen**.

19.3.9.5 VPN - Wie Sie eine Regel ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.

3) Navigieren Sie im Menübaum zu **VPN > Regeln > Konfigurierte Regeln**.

4) Markieren Sie die Regel im Menübaum, die Sie ändern möchten.

5) Geben Sie unter **Priorität** die Priorität ein.

6) Geben Sie unter **Dienst** den Dienst (z. B. DNS) ein.

7) Geben Sie unter **Aktion für die Regel** die Regel (**PASS**, **PASS_INCOMING**, **PASS_OUTGOING**, **DENY**) ein.

8) Aktivieren Sie ggf. das Kontrollkästchen **Verschlüsselung erforderlich**.

9) Aktivieren Sie das Kontrollkästchen **Regel aktivieren**.

10) Geben Sie unter **Quelladresse** den **Typ** und die **IP-Adresse** für die geänderte Regel ein.

11) Geben Sie unter **Zieladresse** den **Typ** und die **IP-Adresse** für die geänderte Regel ein.

12) Nach der gesamten VPN-Konfiguration wird die Änderung mit **Aktivieren der konfigurierten VPN Tabellen** übernommen

19.3.9.6 VPN - Wie Sie eine Regel für die Gegenrichtung hinzufügen

Wenn eine IPsec-Regel für eine Übertragungsrichtung angelegt ist, sollte gleich danach die Regel für die Gegenrichtung hinzufügt werden. Mit der Funktion „Regel für die Gegenrichtung hinzufügen“ werden die Einträge der ausgewählten Regel übernommen, wobei Quell- und Zieladresse gegeneinander getauscht und die Tunnelzuordnung entsprechend gewechselt wird.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.

3) Navigieren Sie im Menübaum zu **VPN > Regeln > Konfigurierte Regeln**.

4) Markieren Sie die Regel im Menübaum, die Sie bearbeiten möchten.

5) Klicken Sie auf die Registerkarte **Regel für Gegenrichtung hinzufügen**.

6) Klicken Sie auf **Übernehmen**.

7) Nach der gesamten VPN-Konfiguration wird die Änderung mit **Aktivieren der konfigurierten VPN Tabellen** übernommen

19.3.9.7 VPN - Wie Sie eine Regel löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.

3) Navigieren Sie im Menübaum zu **VPN > Regeln > Konfigurierte Regeln**.

4) Markieren Sie im Menübaum die Regel, die Sie löschen möchten.

5) Klicken Sie auf die Registerkarte **Regel löschen**. Die ausgewählte Regel mit allen Daten wird angezeigt.

6) Klicken Sie auf **Löschen**. Es erscheint eine Warnung, dass Sie im Begriff sind diese Regel zu löschen.

7) Nach der gesamten VPN-Konfiguration wird die Änderung mit **Aktivieren der konfigurierten VPN Tabellen** übernommen

19.3.10 PKI-Server

Der PKI-Server bezeichnet einen Server, der digitale Zertifikate ausstellen, verteilen und prüfen kann. Die innerhalb einer PKI (Public Key Infrastruktur) ausgestellten Zertifikate werden zur Absicherung der Kommunikation verwendet.

Über die vom PKI-Server konfigurierte PKI-URL wird bei Verwendung von Zertifikaten (digitalen Signaturen) versucht, die CRL herunterzuladen.

19.3.10.1 VPN - Wie Sie den PKI-Server anzeigen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.
3) Navigieren Sie im Menübaum zu **VPN > Public Key Infrastructure (PKI)**.
4) Klicken Sie auf die Registerkarte **PKI-Server anzeigen**. Es werden Ihnen der **Name des PKI-Servers**, der **PKI-Servertyp** und die **URL des PKI-Servers** angezeigt.

19.3.10.2 VPN - Wie Sie einen PKI-Server hinzufügen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.
3) Navigieren Sie im Menübaum zu **VPN > Public Key Infrastructure (PKI)**.
4) Klicken Sie auf die Registerkarte **PKI-Server hinzufügen**.
5) Geben Sie den **Namen des PKI-Servers** an.
6) Geben Sie den **PKI-Servertyp** (z. B. LDAP) an.
7) Geben Sie die **URL des PKI-Servers** ein.
8) Bestätigen Sie und klicken auf **Übernehmen**.

19.4 Zertifikatshandling

Das Zertifikatshandling (für Secure Sockets Layer SSL) ermöglicht die gesicherte Administration des Kommunikationssystems. Die Daten können nicht von unberechtigten Stellen gelesen bzw. manipuliert werden. Die Autorisierung erfolgt über Zertifikate. Zertifikate können Sie generieren und verwalten.

Der Administrationszugriff erfolgt verschlüsselt über HTTPS unter Verwendung des SSL/TLS - Protokolls. Zertifikate dienen zur Authentifizierung des Kommunikationssystems. Standardmäßig wird ein selbstsigniertes Zertifikat verwendet. Zur Erhöhung der Sicherheit kann ein Kundenspezifisches Zertifikat verwendet werden.

SSL stellt folgende Sicherungsdienste zur Verfügung:

- Authentizität (der Kommunikationspartner ist der, der er zu sein vorgibt)
- Vertraulichkeit (die Daten können von einem Dritten nicht gelesen werden)
- Integrität (die Daten wurden so empfangen, wie sie gesendet wurden)

Diese Sicherungsdienste erfordern eine vorherige Verständigung auf einen Sicherheitsmechanismus und den Austausch von kryptographischen Schlüsseln. Diese beiden Aufgaben werden beim Verbindungsaufbau erledigt.

SSL verwendet Zertifikate und Schlüssel, um eine gesicherte Datenübertragung zu ermöglichen.

CRL (Certificate Revocation Lists)

Certificate Revocation Lists (CRL) sind Dateien, welche eine Liste gesperrter Zertifikate, ihrer Seriennummer und ihrer Sperr-Daten enthält. Außerdem enthält eine CRL-Liste den Namen des Ausstellers der Zertifikationsperrliste und des nächsten Aktualisierungszeitpunkts.

CDP (CRL Distribution Point)

CRL Distribution Point (CDP) ist das Verzeichnis (der Ort, in welchem die aktuelle Version der CRLs liegt (z. B. http://sectestcal.microsoft.com/ErtEnvoll/SecTestCAL.crl).

Systemspezifische Informationen

Bei SSL-basierter Administration findet eine Client-Server-Kommunikation statt.

Der Server authentifiziert sich gegenüber dem Client mit Hilfe der im WBM generierten oder importierten Zertifikate. Im Browser kann ein solches Zertifikat als vertrauliches Zertifikat importiert werden, um Warnmeldungen des Browsers beim Verbinden zum SSL-Server zu vermeiden.

INFO: Die SSL-Zertifikatsgenerierung kann auch für SPE verwendet werden.

19.4.1 Wie Sie ein CA-Zertifikat generieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.

3) Navigieren Sie im Menübaum zu **SSL > Zertifikatsgenerierung**.

4) Klicken Sie auf die Registerkarte **CA-Zertifikat generieren**.

5) Vergeben Sie den **Name des Zertifikats**.

6) Vergeben Sie ebenfalls eine laufende Nummer im Feld **Seriennummer des Zertifikats**.

7) Wählen Sie unter **Signatur-Algorithmus-Typ** (**sha1RSA**, **md5RSA**, **sha256RSA**, **sha512RSA**) den Algorithmus aus.

8) Wählen Sie unter **Länge des öffentl. Schlüssels** (1024, 1536, 2048) den öffentlichen Schlüssel aus.

9) Geben Sie in den entsprechenden Feldern den Beginn und das Ende der Zertifikatsgültigkeit ein.

10) Füllen Sie anschließend die Felder zum **Antragsteller** bzw. **Alternativer Antragstellername** aus.

11) Tragen Sie den **CRL-Verteilungspunkt** ein.

12) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

19.4.2 Wie Sie ein selbstsigniertes Zertifikat generieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.

3) Navigieren Sie im Menübaum zu **SSL > Zertifikatsgenerierung**.

4) Klicken Sie auf die Registerkarte **Selbstsigniertes Zertifikat generieren** im Fenster **Zertifikatsgenerierung**.

5) Vergeben Sie im Feld **Name des Zertifikats** einen Namen für das generierte Zertifikat.

6) Vergeben Sie ebenfalls eine laufende Nummer im Feld **Seriennummer des Zertifikats**.

7) Wählen Sie unter **Signatur-Algorithmus-Typ** den Algorithmus aus.

8) Wählen Sie unter **Länge des öffentl. Schlüssels** den öffentlichen Schlüssel aus.

9) Geben Sie in den entsprechenden Feldern den Beginn und das Ende der Zertifikatsgültigkeit ein.

10) Füllen Sie anschließend die Felder zum **Antragsteller** bzw. **Alternativer Antragstellername** aus.

11) Tragen Sie den **CRL-Verteilungspunkt** ein.

12) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

19.4.3 Wie Sie eine Zertifikatsanforderung (CSR) generieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.

3) Navigieren Sie im Menübaum zu **SSL > Zertifikatsverwaltung > Server-Zertifikate**.

4) Geben Sie in der Registerkarte **Zertifikatsanforderung (CSR) generieren** den Namen der Zertifikatsanforderung ein.

5) Geben Sie den **Signatur-Algorithmus-Typ** ein.

6) Geben Sie die **Länge des öffentl. Schlüssels** ein.

7) Geben Sie die Angaben zum **Antragsteller** bzw. für einen **Alternativen Antragsteller** ein.

8) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

19.4.4 Wie Sie ein Server-Zertifikat importieren (PKCS#12)

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.

3) Navigieren Sie im Menübaum zu **SSL > Zertifikatsverwaltung > Server-Zertifikate**.

4) Klicken Sie auf die Registerkarte **Server-Zertifikat importieren (PKCS#12)** im Fenster **Server-Zertifikate**.

5) Geben Sie den **Name des Zertifikats** ein.

6) Geben Sie das **Entschlüsselungskennwort** ein.

7) Geben Sie unter **Datei mit dem Zertifikat** die gewünschte Zertifikatsdatei mit Hilfe von **Durchsuchen** ein.

8) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

19.4.5 Wie Sie Zertifikate anzeigen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.

3) Navigieren Sie im Menübaum zu **SSL > Zertifikatsverwaltung > Server-Zertifikate**.

4) Klicken Sie auf das gewünschte Zertifikat. Das Fenster **Server-Zertifikate** erscheint.

5) Klicken Sie auf die Registerkarte **Zertifikat anzeigen** und Sie können das aktuelle Zertifikat ansehen.

19.4.6 Wie Sie ein Zertifikat löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.

3) Navigieren Sie im Menübaum zu **SSL > Zertifikatsverwaltung > Server-Zertifikate**.

4) Klicken Sie auf das gewünschte Zertifikat. Das Fenster **Server-Zertifikate** erscheint.

5) Klicken Sie auf die Registerkarte **Zertifikat löschen**. Der Name des aktuell gültigen Zertifikats wird angezeigt mit der Warnung, dass Sie im Begriff sind dieses zu löschen.

6) Wenn Sie das Zertifikat wirklich löschen wollen, klicken Sie auf **Löschen**.

19.4.7 Wie Sie ein Zertifikat exportieren (X.509)

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.

3) Navigieren Sie im Menübaum zu **SSL > Zertifikatsverwaltung > Server-Zertifikate**.

4) Klicken Sie auf das gewünschte Zertifikat. Das Fenster **Server-Zertifikate** erscheint.

5) Klicken Sie auf die Registerkarte **Zertifikat exportieren (X.509)**. Sie können das Zertifikat öffnen oder speichern.

19.4.8 Wie Sie ein verlängertes Zertifikat importieren (X.509)

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.

3) Navigieren Sie im Menübaum zu **SSL > Zertifikatsverwaltung > Server-Zertifikate**.

4) Klicken Sie auf das gewünschte Zertifikat. Das Fenster **Server-Zertifikate** erscheint.

5) Klicken Sie auf die Registerkarte **Verlängertes Zertifikat importieren (X.509)**. Der Name des aktuell gültigen Zertifikats wird angezeigt.

6) Im Feld **Datei mit dem Zertifikat** geben Sie das gewünschte Zertifikat ein oder wählen es über das Feld **Durchsuchen** aus.

7) Beenden Sie Ihre Eingabe mit **Fingerabdruck des**.

19.4.9 Wie Sie ein Zertifikat aktivieren

Mit dieser Funktion legen sie das zu verwendende Zertifikat für die web-basierte Administration fest.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.

3) Navigieren Sie im Menübaum zu **SSL > Zertifikatsverwaltung > Server-Zertifikate**.

4) Klicken Sie auf das gewünschte Zertifikat.

5) Klicken Sie auf die Registerkarte **Zertifikat aktivieren**. Es erscheint eine Warnung, dass diese Aktion alle bestehenden HTTP-Verbindungen unterbricht.

6) Wählen Sie aus der Aufklappliste **System** das gewünschte System aus (OpenScape Business, UC Booster Server, UC Booster Card), für das Sie das Zertifikat aktivieren wollen.

> ***INFO:*** Für eine korrekte Funktion muss in jedem Zertifikat im Feld **Allgemeiner Name** die IP-Adresse des Systems eingetragen sein. Achten Sie darauf, dass Sie das richtige Zertifikat für das ausgewählte System aktivieren.

7) Klicken Sie auf **Sofort aktivieren**.

19.5 Web-Sicherheit

Unter Web-Sicherheit finden Sie den Web-Zugriffs-Filter, mit dem Sie Berechtigungen für Clients steuern, und das Admin-Protokoll über das Sie Recherchen über Zugriffe und Änderungen am Kommunikationssystem nachverfolgen können.

19.5.1 Verbindungen zum Web-Server

Die Verbindungen der Clients (z. B. myPortal for Mobile/Tablet) zum internen Web-Server des Kommunikationssystems können entweder verschlüsselt (HTTPS) oder unverschlüsselt (HTTP) erfolgen.

HINWEIS: Unverschlüsselte Verbindungen zum Web-Server können Unbefugten den Zugriff auf sensible Daten ermöglichen! Aus Sicherheitsgründen wird dringend empfohlen, bei Nutzung von myPortal for Mobile/Tablet über Internet nur eine verschlüsselte Verbindung (HTTPS) zu nutzen.

Für myPortal to go steht nur eine verschlüsselte Verbindung zum Web-Server zur Verfügung.

Für myPortal for OpenStage (XML) ist das Freischalten der unverschlüsselten Verbindung (HTTP) notwendig.

19.5.1.1 Wie Sie die Verbindungen zum Web-Server konfigurieren (UC Suite)

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Sicherheit**.

3) Navigieren Sie im Menübaum zu **Web-Zugriff**.

4) Konfigurieren Sie die Verbindungen zum Web-Server:

- Wenn Sie verschlüsselte Verbindungen erlauben möchten, aktivieren Sie das Kontrollkästchen **HTTPS**.
- Wenn Sie unverschlüsselte Verbindungen erlauben möchten, aktivieren Sie das Kontrollkästchen **HTTP**.

5) Aktivieren Sie ggf. das Feld **Anmeldedaten im Endgerät speichern**, wenn Sie diese Funktion zulassen wollen. Hiermit werden über sogenannte Cookies die Anmeldedaten im Web-Browser des Mobiltelefons gespeichert.

6) Klicken Sie auf **Speichern**.

19.5.1.2 Wie Sie die Verbindungen zum Web-Server konfigurieren (UC Smart)

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Applikationen > UC Smart > Grundeinstellungen**.

3) Prüfen Sie, ob UC Smart **Aktiv** ist.

4) Konfigurieren Sie die Verbindungen zum Web-Server:

- Wenn Sie verschlüsselte Verbindungen erlauben möchten, aktivieren Sie das Kontrollkästchen **HTTPS**.
- Wenn Sie unverschlüsselte Verbindungen erlauben möchten, aktivieren Sie das Kontrollkästchen **HTTP**.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

19.5.2 Admin-Protokoll

Das Admin-Protokoll bietet die Möglichkeit zu erfahren, wann welche Änderungen am Kommunikationssystem durchgeführt worden sind und von wem diese gemacht wurden.

19.5.2.1 Wie Sie das Admin.-Protokoll laden

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung**.

3) Navigieren Sie im Menübaum zu **Admin.-Protokoll > Admin.-Protokoll-Daten**.

4) Im Fenster **Admin.-Protokoll-Daten** erscheint die Meldung "Das Admin-Log wird vom System geladen. Bitte bestätigen".

5) Klicken Sie auf **Laden**.

19.5.2.2 Wie Sie die Admin.-Protokoll-Sprache ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Wartung**.

3) Navigieren Sie im Menübaum zu **Admin.-Protokoll > Konfiguration**.

4) Stellen Sie im Fenster **Konfiguration ändern** unter **Admin.-Protokoll-Sprache** die gewünschte Sprache ein.

5) Klicken Sie auf **Übernehmen**.

19.6 Schutz vor SIP-Attacken (SIP Attack Protection)

Sogenannte SIP-Attacken stellen eine neue Form der Angriffe auf Kommunikationssysteme über die IP-Telefonie dar. Angriffe können entweder aus dem LAN als auch über das Internet (via falsch konfigurierte Router) erfolgen. Schutz vor SIP-Attacken bietet ein passwortgeschützter SIP-Zugang.

Für einen SIP-Teilnehmerzugang sollten folgende Regeln gelten:

- Aktive Authentifikation
- Ein qualifiziertes Passwort, das
  - zwischen 8 und 20 Zeichen lang ist,
  - einen oder mehrere Großbuchstaben enthält (A bis Z),
  - einen oder mehrere Kleinbuchstaben enthält (a bis z),
  - eine oder mehrere Ziffern enthält (0 bis 9),
  - ein oder mehrere Sonderzeichen enthält (z. B. %),
  - nicht mehr als 3 Zeichen wiederholt.
- Definition einer SIP-Teilnehmer-ID die sich von der Rufnummer unterscheidet.

Wenn ein neuer SIP-Teilnehmer eingerichtet wird, ist standardmäßig die Authentifikation aktiviert und ein zufälliges Passwort wird generiert. Da dieses zufällige Passwort nicht bekannt ist, muss es vom Administrator geändert werden.

Im Kommunikationssystem werden die entsprechenden Einstellungen über den Wizard "Zentrale Telefonie" gemacht bzw. über den Manager E.

Während des Systemstarts wird die Passwortliste geprüft und ein EventLog-Eintrag (Ereignisanzeige) gemacht, falls ein SIP-Teilnehmer ohne Passwort konfiguriert wurde.

INFO: Wenn das Kommunikationssystem als Internet Router genutzt wird, muss Port 5060 geschlossen sein (Standardeinstellung). Bei Internettelefonie über ITSP öffnet das Kommunikationssystem die relevanten Ports und hält diese offen.

Auch wenn ein externer Router bzw. Firewall genutzt wird, muss Port 5060 geschlossen sein. Es liegt in der Verantwortung des Kommunikationssystems diesen Port (falls benötigt) zu öffnen.

---

20 Vernetzung von OpenScape Business

OpenScape Business Kommunikationssysteme können untereinander vernetzt werden und zusätzlich auch mit den Kommunikationssystemen OpenScape 4000 (HiPath 4000) und OpenScape Voice. Bei einer homogenen OpenScape Business Vernetzung können Teilnehmer Leistungsmerkmale wie Anwesenheitsstatus, Voicemail, Konferenzen und vieles mehr so nutzen, wie dies bislang nur in einem einzelnen OpenScape Business Kommunikationssystem der Fall war.

Mögliche Vernetzungen:

- Reine Sprachvernetzung von OpenScape Business X
- OpenScape Business X Vernetzung (optional mit UC Suite oder UC Smart) und OpenScape Business S (immer mit UC Suite).
- OpenScape Business X mit OpenScape 4000/HiPath 4000 (UC-Funktionalität bei OpenScape Business nur unter bestimmten Voraussetzungen)
- OpenScape Business X mit OpenScape Voice (ohne UC-Funktionalität bei OpenScape Business)
- Anbindung von externen Anschaltungen an OpenScape Business über SIP-Interconnection.
- Vernetzung über ISDN
- OpenScape Business Netzverbund mit zentralem ITSP-Amtsanschluss

Die Kommunikationssysteme werden mit dem Wizard **Vernetzungs-Konfiguration** für die Vernetzung vorbereitet. In diesem Wizard wird angegeben, ob es sich um einen Master- oder Slave-Knoten handelt. Zusätzlich werden der Richtung 16 (Networking) automatisch 16 Leitungen zugeordnet.

Alle Vernetzungen, die Unified Communications Leistungsmerkmale nutzen (wie z.B. UC Smart oder UC Suite, Application Launcher, Gate View, Open Directory Service), müssen auf einem geschlossenen Rufnummernplan aufsetzen. Vernetzungen ohne Unified Communications Leistungsmerkmale können auf einem offenen oder geschlossenen Rufnummernplan basieren. Um flexibel auf Erweiterungswünsche von Kunden reagieren zu können, wird empfohlen, bei einem neu angelegten Netzverbund immer die geschlossene Nummerierung zu nutzen.

INFO: Die Einrichtung einer IP-Vernetzung ist ein komplexes Thema und sollte nur von erfahrenen Servicetechnikern durchgeführt werden.

Ein reiner OpenScape Business X1 Netzverbund ist nicht möglich, da ein X1-System kein Master-System sein kann und es im Netzverbund immer ein Master-System geben muss.

Eine Vernetzung von OpenScape Business mit folgenden Systemen wird nicht unterstützt:

- HiPath 3000
- HiPath 5000 RSM
- OpenScape Office MX

- OpenScape Office LX

Die Migration einer HiPath 3000 (inklusive HiPath 5000 RSM) nach OpenScape Business ist im Kapitel *Migration* beschrieben.

20.1 Vernetzungsplan

Bevor ein Netzverbund eingerichtet wird, sollte in Absprache mit dem Kunden ein Vernetzungsplan erstellt werden.

Der Vernetzungsplan sollte folgende Daten enthalten:

- Knoten-ID (Node-ID) und zugehörige IP-Adressen
- Rufnummernplan

20.1.1 Homogene und inhomogene Netze

Generell wird bei der Vernetzung zwischen homogenen (alle Komponenten gehören zu einer einzigen Systemfamilie) und inhomogenen Netzen (unterschiedliche Komponenten) unterschieden.

Homogenes Netz (Natives Netzwerk)

Ein homogenes (natives) Netz besteht aus Komponenten der OpenScape Business Systemfamilie.

Inhomogenes Netz (Hybrides Netzwerk)

Ein inhomogenes (hybrides) Netz besteht aus Komponenten der Systemfamilie OpenScape Business und z. B. einer OpenScape 4000 oder einer OpenScape Voice.

Übersicht aller OpenScape Business Knoten im Netzverbund

Über den Eintrag **Netzwerk** in der Navigationsleiste können alle OpenScape Business Konten eines Netzverbundes angezeigt werden. Zusätzlich können auch alle OpenScape Business Teilnehmer des Netzverbundes nach Knoten sortiert angezeigt werden.

Folgende Informationen können in der Ansicht **Knoten-Sicht** angezeigt werden:

- **Knoten-ID**: Knoten-ID
- **M** / **S**: Kennzeichnung, ob der Knoten Master oder Slave ist
- **Netzwerkname**: Name des Knotens
- **Typ**: Typ des Knotens (**OSBiz X**: Hardware-Modell, **OSBiz S**: Softswitch)
- **OSBiz X / OSBiz S**: IP-Adresse des Knotens, klickbar (öffnet das WBM des Knotens)
- **Application Server**: IP-Adresse des UC Servers
- **Registrierungsstatus**: Status der Registrierung
- **Aktiv**: Anzeige, ob der Knoten aktiv ist oder nicht

Folgende Informationen können in der Ansicht **Rufnummern** angezeigt werden:

- **Rufnummer**: Rufnummer des Teilnehmers
- **DuWa**: Durchwahlnummer des Teilnehmers
- **Name**: Name des Teilnehmers
- **Port-Typ**: Typ des zugeordneten Telefons
- **Knoten**: Knoten-ID des Knotens, an dem der Teilnehmer angeschlossen ist

20.1.1.1 Wie Sie die Übersicht aller OpenScape Business Knoten anzeigen

Voraussetzungen

- Mehrere OpenScape Business Kommunikationssysteme sind miteinander vernetzt.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Netzwerk**.

2) Klicken Sie im Navigationsbaum auf **Knoten-Sicht**. Es sind alle OpenScape Business Knoten im Netzverbund aufgelistet.

20.1.1.2 Wie Sie die Teilnehmer aller OpenScape Business Knoten anzeigen

Voraussetzungen

- Mehrere OpenScape Business Kommunikationssysteme sind miteinander vernetzt.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Netzwerk**.

2) Klicken Sie im Navigationsbaum auf **Rufnummern**. Es sind die Teilnehmer aller OpenScape Business Knoten im Netzverbund aufgelistet.

3) Über die Einträge einer Aufklappliste können Sie die Liste nach unterschiedlichen Kriterien sortieren.

20.1.1.3 Wie Sie Teilnehmer über alle OpenScape Business Knoten suchen

Voraussetzungen

- Mehrere OpenScape Business Kommunikationssysteme sind miteinander vernetzt.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Netzwerk**.

2) Klicken Sie im Navigationsbaum auf **Rufnummern**. Es sind die Teilnehmer aller OpenScape Business Knoten im Netzverbund aufgelistet.

3) Geben Sie in dem gewünschten Feld Ihr Suchkriterium ein und klicken Sie auf **Suchen**. Alle gefundenen Einträge werden angezeigt.

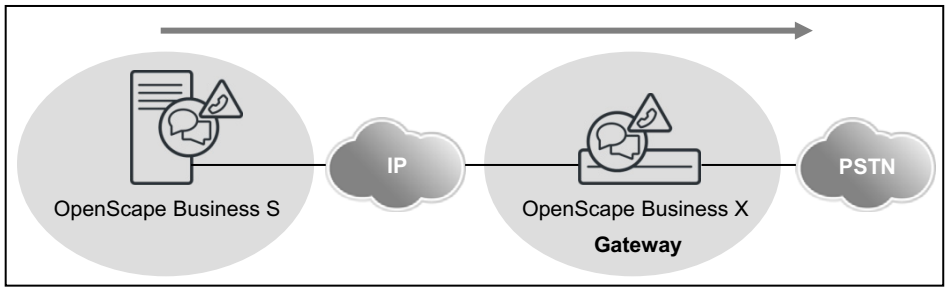
4) Über die Einträge einer Aufklappliste können Sie Ihre Suchergebnisse nach unterschiedlichen Kriterien sortieren.

20.1.2 Single- und Multi-Gateway

Bei einer homogenen Vernetzung von OpenScape Business wird zwischen Single- und Multi-Gateway unterschieden, wobei Single-Gateway die Vernetzung mit einem einzigen Gateway und Multi-Gateway die Vernetzung mit mehreren Gateways beschreibt.

Single-Gateway

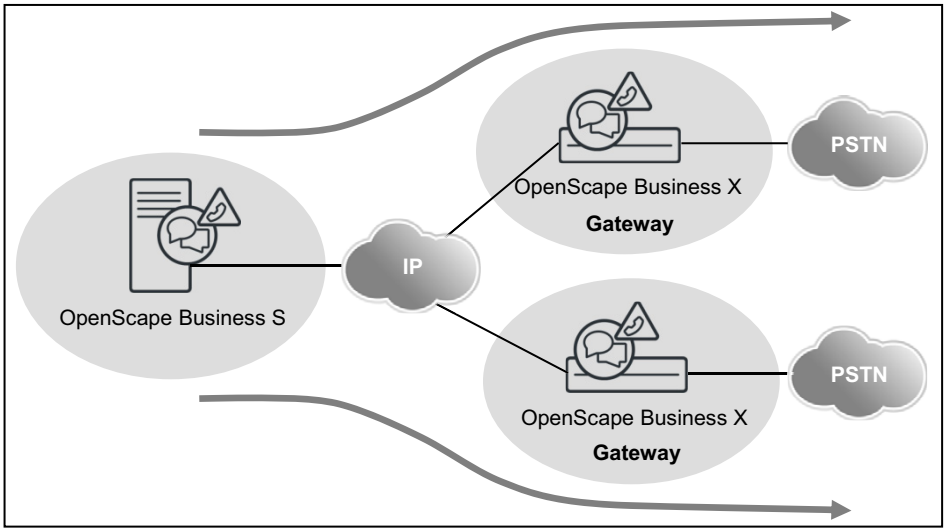
Bei einer Single-Gateway-Vernetzung werden die Anrufe vom und zum Server über ein einziges Gateway geroutet. Alle IP-Teilnehmer, die am Server registriert sind, nutzen dieses eine Gateway.



- Wird unterstützt, wenn sich ein oder mehrere OpenScape Business S im Netzwerk befinden.
- Die IP-Teilnehmer sind an den unterschiedlichen Kommunikationssystemen angeschlossen.
- OpenScape Business X wird als Gateway genutzt.

Multi-Gateway

Bei einer Multi-Gateway-Vernetzung werden die Anrufe über mehrere, verschiedene OpenScape Business Gateways geroutet.



- Nur 1 PSTN-Provider bzw. eine Amtsrufnummer pro Gateway
- Die Teilnehmer unterschiedlicher Standorte sind an einem zentralen System (OpenScape Business) registriert.
- Jedem Teilnehmer der OpenScape Business S wird ein bestimmtes Gateway (OpenScape Business X) zugeordnet.
- Es darf nur eine einzige OpenScape Business S im Netzwerk befinden.
- OpenScape Business und OpenScape Business S befinden sich in derselben Zeitzone und im gleichen Land (gleicher Country-Code).
- Es gibt nur eine Amtskennzahl netzweit.
- An den Gateways können z. B. ISDN- und analoge Teilnehmer lokal eingerichtet sein.

20.2 Netzweite Leistungsmerkmale

Netzweite Voice-Leistungsmerkmale werden im wesentlichen bestimmt durch das SIP-Q-Vernetzungsprotokoll. Netzweite UC-Leistungsmerkmale werden bestimmt durch die Vernetzung der UC Suite und deren Clients. UC-Smart bietet keine netzweite UC.

20.2.1 Netzweite Leistungsmerkmale der UC Suite

Die folgende Tabelle bietet Ihnen einen Überblick über die netzweiten Leistungsmerkmale der UC Suite und deren Clients und das Interworking mit anderen Kommunikationssystemen.

myPortal for Desktop

Unified Communication Leistungsmerkmale	Homogene OpenScape Business Vernetzung	Inhomogene Vernetzung	
		OpenScape 4000	OpenScape Voice
Verzeichnisse	Persönliches Verzeichnis	-	-
	Internes Verzeichnis netzweit	-	-
	Externes Verzeichnis (jeweils lokal per .csv-Import, lokale Suche)	-	-
	Externes Offline-Verzeichnis (zentral per LDAP)	-	-
Favoriten-Liste	Interne Teilnehmer (OpenScape Business X und OpenScape Business S) und externe Teilnehmer	-	-
Journal	Offen, Alle Anrufe, Entgangen, Angenommen, Intern, Extern, Ankommend, Gehend, Geplant	-	-
PopUp-Fenster	Kommender Ruf	-	-
	Gehender Ruf	-	-
	Neue Sprachnachricht	-	-
	Ändern des eigenen Anwesenheitsstatus	-	-
	Öffnen des persönlichen Kontakts bei kommendem Ruf	-	-
	Öffnen einer eMail	-	-
	Anrufe planen	-	-
Mitschneiden von Gesprächen	Ja	-	-
Anwesenheitsstatus	Ja	-	-
Besetztstatus	Ja	-	-
CallMe-Dienst	Ja	-	-
Statusbezogene Anrufumleitung	Ja	-	-
Persönlicher und Zentraler AutoAttendant	Ja	-	-
Instant Messaging	Ja	-	-
Multi User Chat	Ja	-	-
Sprachbox für Sprachnachrichten und Faxe	Ja	-	-
Sprachnachrichten	Ja	-	-
Fax (kommend und gehend)	Ja	-	-

Unified Communication Leistungsmerkmale	Homogene OpenScape Business Vernetzung	Inhomogene Vernetzung	
		OpenScape 4000	OpenScape Voice
Computer Telephony Integration CTI	Ja	-	-
Konferenzen	Ja	-	-
Desktop Wahl	Ja	-	-

myPortal for Outlook

Unified Communication Leistungsmerkmale	Homogene OpenScape Business Vernetzung	Inhomogene Vernetzung	
		OpenScape 4000	OpenScape Voice
Verzeichnisse	Internes Verzeichnis netzweit	-	-
	Externes Verzeichnis (jeweils lokal per .csv-Import, lokale Suche)	-	-
	Externes Offline-Verzeichnis (zentral per LDAP)	-	-
Favoriten-Liste	Interne Teilnehmer (OpenScape Business X und OpenScape Business S) und externe Teilnehmer	-	-
Journal	Offen, Alle Anrufe, Entgangen, Angenommen, Intern, Extern, Ankommend, Gehend, Geplant	-	-
PopUp-Fenster	Kommender Ruf	-	-
	Gehender Ruf	-	-
	Neue Sprachnachricht	-	-
	Ändern des eigenen Anwesenheitsstatus	-	-
	Öffnen des persönlichen Kontakts bei kommendem Ruf	-	-
	Öffnen einer eMail	-	-
	Anrufe planen	-	-
Mitschneiden von Gesprächen	Ja	-	-
Anwesenheitsstatus	Ja	-	-
Besetztstatus	Ja	-	-
CallMe-Dienst	Ja	-	-
Statusbezogene Anrufumleitung	Ja	-	-
Persönlicher und Zentraler AutoAttendant	Ja	-	-
Instant Messaging	Ja	-	-
Multi User Chat	Ja	-	-

Unified Communication Leistungsmerkmale	Homogene OpenScape Business Vernetzung	Inhomogene Vernetzung	
		OpenScape 4000	OpenScape Voice
Sprachbox für Sprachnachrichten und Faxe	Ja	-	-
Sprachnachrichten	Ja	-	-
Fax (kommend und gehend)	Ja	-	-
Computer Telephony Integration CTI	Ja	-	-
Konferenzen	Ja	-	-
Desktop Wahl	Ja	-	-

myAttendant

Unified Communication Leistungsmerkmale	Homogene OpenScape Business Vernetzung	Inhomogene Vernetzung	
		OpenScape 4000	OpenScape Voice
Komfortable Anrufvermittlung	Ja	-	-
Verzeichnisse	Persönliches Verzeichnis	-	-
	Internes Verzeichnis netzweit	-	-
	Externes Verzeichnis (jeweils lokal per .csv-Import, lokale Suche)	-	-
	Externes Offline-Verzeichnis (zentral per LDAP)	-	-
Suche in internem Verzeichnis	Ja	-	-
Teilnehmerverwaltung	Ja	-	-
Journal	Offen, Alle Anrufe, Entgangen, Angenommen, Intern, Extern, Ankommend, Gehend, Geplant	-	-
Message Center	Nein	-	-
Anwesenheitsstatus sehen	Ja	-	-
Anwesenheitsstatus für Teilnehmer ändern	Ja	-	-
Mitschneiden von Gesprächen	Ja	-	-
Multi-User Chat	Ja	-	-
PopUp-Fenster	Kommender Ruf, Annahme des kommenden Rufes	-	-
Sofortnachrichten (Instand Messages) senden	Ja	-	-

myPortal for Mobile

Unified Communication Leistungsmerkmale	Homogene OpenScape Business Vernetzung	Inhomogene Vernetzung	
		OpenScape 4000	OpenScape Voice
Verzeichnisse	Internes Telefonbuch mit Anwesenheitsstatus netzweit	-	-
	Persönliche Kontakte	-	-
	System Telefonbuch	-	-
	Externes Offline-Verzeichnis (zentral per LDAP)	-	-
Favoritenliste	Interne und externe Teilnehmer	-	-
Journal	Kommende Rufe, Gehende Rufe, Manuelle Wahl, Wahlwiederholung	-	-
Sprachbox	Ja	-	-
Anwesenheitsstatus	Ja	-	-

myPortal for OpenStage

Unified Communication Leistungsmerkmale	Homogene OpenScape Business Vernetzung	Inhomogene Vernetzung	
		OpenScape 4000	OpenScape Voice
Anwesenheitsstatus	Ja	-	-
Sprachbox	Ja	-	-

myAgent

Unified Communication Leistungsmerkmale	Homogene OpenScape Business Vernetzung	Inhomogene Vernetzung	
		OpenScape 4000	OpenScape Voice
Alle Leistungsmerkmale	Lokale Anschaltung myAgents-Clients und Contact-Center-Optionen pro OpenScape Business-Netzknoten. Über abgesetzte Teilnehmer oder VPN-Anschaltungen von Teilnehmern sind standortübergreifende Contact-Center-Lösungen möglich.	-	-

myReports

Unified Communication Leistungsmerkmale	Homogene OpenScape Business Vernetzung	Inhomogene Vernetzung	
		OpenScape 4000	OpenScape Voice
Alle Leistungsmerkmale	Lokale Anschaltung myAgents-Clients und Contact-Center-Optionen pro OpenScape Business-Netzknoten. Über abgesetzte Teilnehmer oder VPN-Anschaltungen von Teilnehmern sind standortübergreifende Contact-Center-Lösungen möglich.	-	-

20.2.2 Netzweite Voice-Leistungsmerkmale

Bei einer Vernetzung über das SIP-Q-Protokoll werden folgende Sprachleistungsmerkmale für OpenScape Business und andere Kommunikationssysteme unterstützt.

Leistungsmerkmal	SIP-Q (IP-Netzwerk)
Basic Call	Ja
Rückruf bei Besetzt	Ja
Rückruf im Freifall	Ja
Aufschalten	Ja
Anklopfen	Ja
Zweitanruf	Ja
Calling Line Identification Presentation CLIP	Ja
Calling Line Identification Restriction CLIR	Ja
Connected Line Identification Presentation COLP	Ja
Connected Line Identification Restriction COLR	Ja
Calling / Connected Name Identification Presentation CNIP	Ja
Calling / Connected Name Identification Restriction CNIR	Ja
Anrufschutz	Ja
Anrufumleitung	Ja
Rufweiterschaltung im Besetztfall	Ja
Rufweiterschaltung im Freifall	Ja
Call Deflection	Ja
Advice of Charge at Call Setup	Nein
Advice of Charge during Call	Ja
Advice of Charge at the end of the call	Ja

Leistungsmerkmal	SIP-Q (IP-Netzwerk)
Wegeoptimierung	Ja
Rerouting	Nein
Message Waiting Indication / Info	Ja
Fangen	Ja
Halten	Ja
Makeln	Ja
Transfer	Ja
Konferenz	Ja
Wiederanruf	Ja
Notruf	Ja
Abwurf	Ja
Private Numbering Plan PNP	Nein
Anrufübernahme	Nein
Sammelanschluss	Ja
SPE (außer bei Konferenz und Applikationen)	Ja

20.3 Lizenzierung eines Netzverbundes

Für ein vernetztes Kommunikationssystem kann eine zentrale Lizenzierung ausgewählt werden.

Alle Lizenzen der Einzelsysteme werden zu einer netzweiten Lizenz am Lizenzserver zusammengefasst. Im Netzverbund können die Lizenzen über das WBM den einzelnen Knoten beliebig zugeordnet werden.

Für weitere Informationen siehe *Lizenzierung mehrerer Kommunikationssysteme (Netzverbund)*.

20.4 Anforderungen an die Vernetzung

Um die Qualität der Sprachübertragung sicherzustellen, müssen die verwendeten IP-Netze und das Kommunikationssystem bestimmte Anforderungen erfüllen. Die Sprachqualität und die Zuverlässigkeit der Sprachkommunikation hängt hierbei von der eingesetzten Netzwerktechnik ab.

Netzwerkparameter, Anforderung für LAN und WAN

Paramter	Mindestan-forderung	Bemerkung
Delay (one way)	50 ms	Höhere Werte verschlechtern die Sprach-qualität.
Round Trip Delay	100 ms	Höhere Werte verschlechtern die Sprach-qualität.
Jitter	20 ms	Höhere Werte verschlechtern die Sprach-qualität.
Packet Loss	3 %	Bei Fax- oder Modem-Übertragungen über G.711 sollte der Paketverlust nicht 0,05 % nicht übersteigen (für den Fall, dass kein T.38 möglich ist).
Consecutive Packet Loss	3 with G.711	Höhere Werte verschlechtern die Sprach-qualität.

Empfehlung zur Bandbreitenkalkulation

- Im Netzverbund ist eine Bandbreite von mindestens 256 kBit/s (jeweils in Sende- und Empfangsrichtung) erforderlich.
- Die Bandbreitenkalkulation sollte von maximal 50 % für den Sprachanteil bzgl. der Gesamtbandbreite ausgehen, d. h. zum Beispiel bei einem 1 MBit-WAN sollten maximal 500 KBit/s für Sprache kalkuliert werden. Bei G.711-Codec sind das beispielsweise maximal 5 IP-Trunks.
- Unabhängig davon sind die Netzeigenschaften bzgl. QoS, Delay, Packet Loss etc. zu beachten.

20.4.1 Anforderungen an die LAN-Vernetzung

Um die Qualität der Sprach- und Datenübertragung sicherzustellen, müssen die verwendeten IP-Netze und das Kommunikationssystem bestimmte Anforderungen an das LAN erfüllen.

LAN-Anforderungen

Das Datennetzwerk muss vom Typ Ethernet sein:

- Empfohlen werden Cat.5-Kabel (geschirmte/ungeschirmte mehradrige Kabel bis 100 MHz für den Horizontal- und Steigbereich gemäß EN 50288).
- Unterstützung für QoS: IEEE 802.1p, DiffServ (RFC 2474).
- Alle aktiven LAN-Ports müssen 100 / 1000 MBit/s und Vollduplex-Kommunikation unterstützen.

Jedes Kommunikationssystem muss über einen Switch oder einen dedizierten Port eines Routers angeschlossen sein. Hubs oder Repeater werden nicht unterstützt.

Die VoIP-Anwendung sollte über ein getrenntes VLAN angeschlossen sein um Kollisionen mit anderen Übertragungen zu minimieren. Wenn alle beteiligten Geräte VLAN (nach IEEE 802.1q) unterstützen, kann der gesamte VoIP-Verkehr in ein separates VLAN ausgelagert werden.

Payload-Verbindungen mit RTP (Realtime Transport Protocol) in einer LAN-Umgebung

Die erforderliche Bandbreite für Sprachübertragung in einem IP-Netzwerk lässt sich mit Hilfe der folgenden Tabelle berechnen:

Codec-Typ	Paketierungs-Parameter	Beispiel- größe (ms)	Payload (Bytes)	Ethernet Paket-länge (Bytes)	Payload- Paket (Overhead in Prozent)	Ethernet Load (inkl.) Kopf (kBit/s)
G.711	20	20	160	230	44%	92
G.711	30	30	240	310	29%	82,7
G.711	40	40	320	390	22%	78
G.711	60	60	480	550	15%	73,3
G.729A	1	20	20	90	350%	36
G.729A	2	40	40	110	175%	22
G.729A	3	60	60	130	117%	17,3
RTCP		5000		280		0,4

Der Load im LAN ist jeweils für Sende- und Empfangsrichtung gültig.

Die Berechnung schließt VLAN-Tagging entsprechend IEEE 802 1q ein. Ohne VLAN-Tagging ist die Länge eines Pakets um 4 Bytes kürzer.

Der Overhead berechnet sich wie folgt:

Protokoll	Bytes
RTP-Header	12
UDP-Header	8
IP-Header	20
802.1Q VLAN Tagging	4
MAC (incl. Preamble, FCS)	26
Summe	70

Payload Transport in T.38 LAN-Umgebung:

	Beispielgröße (ms)	Payload (Bytes)	Ethernet Paket-länge (Bytes)	Payload- Paket (Overhead in Pro-zent)	Ethernet Load (inkl.) Kopf (kBit/s)
T.38	30	169	227	34%	60,5

Payload-Verbindungen mit SRTP (Secure Realtime Transport Protocol) in einer LAN-Umgebung:

Codec-Typ	Beispielgröße (ms)	Payload (Bytes)	Ethernet Paket-länge (Bytes)	SRTP-Ethernet Paketlänge (kBit/s)	RTP-Ethernet Paketlänge (kBit/s	Zusätzliche Bandbreite bei SRTP (%)
G.711	20	160	244	97,6	92	6,1
G.711	30	240	324	86,4	82,4	4,5
G.711	40	320	404	80,8	78	3,6
G.711	60	480	564	75,2	73,3	2,5
G.729A	20	20	104	41,6	36	15,6
G.729A	40	40	124	24,8	22	12,7
G.729A	60	60	144	19,2	17,3	10,8

20.4.2 Anforderungen an die WAN-Vernetzung

Um die Qualität der Sprach- und Datenübertragung sicherzustellen, müssen die verwendeten IP-Netze und das Kommunikationssystem bestimmte Anforderungen an das WAN erfüllen.

WAN-Anforderungen

Wenn IP-Telefonie in internen IP-Netzen, die über WAN gekoppelt sind, eingesetzt wird, gelten folgende Anforderungen:

- Die internen IP-Netze (LAN) müssen jeweils über einen WAN-Anschluss mit fester IP-Adresse mit dem Internet verbunden sein.
- Die für die Gespräche benötigte Bandbreite muss jederzeit sowohl für Upload als auch für Download zur Verfügung stehen.
- Die Anzahl der gleichzeitigen IP-Telefon-Verbindungen über WAN wird von der Bandbreite und den verwendeten Audio-Codecs begrenzt. Bei gleicher Bandbreite können bei Verwendung eines Audio-Codecs mit hoher Komprimierung mehr Telefonverbindungen aufgebaut werden.
- Am WAN-Anschluss der OpenScape Business ist kein Modem integriert, d. h. es ist ggf. ein externes Modem erforderlich. (z. B. ein DSL-Modem oder Kabel-Modem).

Für IP-Telefonie über ITSP (Internet-Telefonie-Service-Provider) gelten folgende Randbedingungen:

- Bei Anschlüssen, die nicht QoS-fähig sind, (in der Regel bei ADSL-Anschlüssen) sind Einschränkungen bei der Sprachqualität möglich. Eine gute Sprachqualität wird erzielt, wenn ein nicht QoS-fähiger Internet-Anschluss ausschließlich für Sprachverbindungen zum ITSP genutzt wird.
- Ein externer Router muss zur Sicherstellung der Sprachqualität QoS-Funktionen und Bandbreitenkontrollmechanismen bereitstellen.

Für Payload-Verbindungen mit RTP (Realtime Transport Protocol) in einer WAN-Umgebung errechnen sich folgende Werte:

Codec-Typ	Paketierungs-Parameter	Beispielgröße (ms)	Payload (Bytes)	Paketlänge (Bytes)	Payload-Paket (Overhead in Prozent)	WAN-Load (kBit/s)	Paketlänge mit Compr. Header (Bytes)	WAN-Load mit Compr. Header (Bytes)
G.711	20	20	160	206	29%	82,4	-	-
G.711	30	30	240	286	19%	76,3,7	-	-
G.711	40	40	320	366	14%	73,2	-	-
G.711	60	60	480	526	10%	70,1,3	-	-
G.729A	1	20	20	66	230%	26,4	28	11,2
G.729A	2	40	40	86	115%	17,2	48	9,6
G.729A	3	60	60	106	77%	14,1	68	9,1
RTCP	-	5000	-	230	-	0,4	-	0,4

Payload Transport in T.38 WAN-Umgebung:

	Beispielgröße (ms)	Payload (Bytes)	Paketlänge (Bytes)	Payload- Paket (Overhead in Prozent)	Ethernet Load (inkl.) Kopf (kBit/s)
T.38 (Redundancy 2)	30	169	203	20%	54,1

Der WAN-Load ist für eine Richtung kalkuliert. Da WAN-Kanäle gewöhnlich Kanäle in beide Richtungen beinhalten, ist dies gleichbedeutend mit der erforderlichen Bandbreite für z. B. einen ISDN-Kanal.

Der Overhead berechnet sich wie folgt:

Protokoll	Bytes
RTP-Header	12
UDP-Header	8
IP-Header	20
PPP	6
Summe	46
Compressed Header	8

Für RTP/UDP/IP-Header-Kompression wird gewöhnlich ein „komprimierter Header“ verwendet. Zusätzlich wird alle 5 Sekunden ein voller Header (46 Bytes) gesendet.

Die Daumenregel zum Berechnen der erforderlichen Bandbreite für n parallele VoIP-Verbindungen mit G.711 (ein Frame pro RTP-Paket) lautet:

Bandbreite WAN = n × (82 kBit/s Voice-Payload + 0,4RTPC)

20.4.3 Rufnummernplan im Netz

Der Rufnummernplan ist eine wichtige Voraussetzung für die Vernetzung. Abhängig vom Rufnummernplan gestaltet sich die Konfiguration des Netzverbundes mehr oder weniger aufwändig. Open Scape Business unterstützt im Netzverbund generell die offene und geschlossene Nummerierung, wobei der volle Umfang der UC-Leistungsmerkmale nur bei geschlossener Nummerierung genutzt werden kann.

Verdeckte (geschlossene) Nummerierung

Bei der verdeckten (geschlossenen) Nummerierung wird ein Teilnehmer im Netzverbund eindeutig durch die Teilnehmerrufnummer identifiziert. Jeder Teilnehmer im Netzverbund kann einen anderen Teilnehmer durch direktes Wählen von dessen Rufnummer erreichen.

Die verdeckte Nummerierung hat den Vorteil, dass keine Knotenrufnummer gewählt werden muss, um einen anderen Teilnehmer in einem anderen vernetzten Kommunikationssystem zu erreichen.

Tabelle: Beispiel für verdeckte Nummerierung

	Knoten 1	Knoten 2	Knoten 3	Knoten 4
Rufnummern	100	200	300	400
	101	201	301	401
	102	202	302	402
	103	203	303	403
	104	204	304	404

Offene Nummerierung

Bei der offenen Nummerierung wird ein Teilnehmer eindeutig durch die Knotenrufnummer und die Teilnehmerrufnummer identifiziert. Teilnehmer unterschiedlicher Kommunikationssysteme (Knoten) im Netzverbund können somit die gleiche Teilnehmerrufnummer haben.

Bei der offenen Nummerierung muss zusätzlich zur Rufnummer des Teilnehmers immer die Knotenrufnummer mitgewählt werden. Dafür können die Rufnummernbänder mehrfach verwendet werden, und es sind mehr Rufnummern nutzbar.

Folgende UC-Leistungsmerkmale werden bei einer offenen Nummerierung nicht unterstützt:

- myPortal Smart
- UC-Lösung UC Suite
- Application Launcher
- Web Collaboration
- Open Directory Services
- netzweiter CSP (CSTA Service Provider)
- DSS-Server

- CMD (CSTA Message Dispatcher)

Folgende UC-Leistungsmerkmale werden bei einer offenen Nummerierung lokal unterstützt:

- Smart VoiceMail (Sprachbox)
- Company AutoAttendant (UC Smart)

Tabelle: Beispiel für offene Nummerierung :

	Knoten 1	Knoten 2	Knoten 3	Knoten 4
Knotenrufnummer	95	96	97	98
Rufnummern	100	100	100	100
	101	101	101	101
	102	102	102	102
	103	103	103	103
	104	104	104	104

20.4.3.1 Wahl von öffentlichen Rufnummern im Netz

Unabhängig von geschlossener oder offener Numerierung ist es sinnvoll, sowohl knoteninterne Ziele als auch netzinterne Ziele über öffentliche Rufnummern anzuwählen. (z. B. als UC Client, der Kontakte im voll qualifizierten Format aus Verzeichnissen wählt).

20.5 Wegeoptimierung (Path Replacement)

Mit Hilfe der Wegeoptimierung (Path Replacement) wird bei vernetzten Kommunikationssystemen eine Doppelbelegung von IP-Leitungen vermieden.

Sind mehrere OpenScape Business vernetzt, so kann es zu folgender Problematik kommen: Teilnehmer A ruft Teilnehmer B an, dieser leitet aber seine Anrufe auf Teilnehmer C um. Teilnehmer A und C sind am selben Netzknoten angeschlossen; Teilnehmer B an einem anderen Netzknoten. Daher belegt der Anruf mit Rufumleitung zunächst zwei Leitungen zwischen den beiden Netzknoten. Um diese Doppelbelegung zu vermeiden sollte die Wegeoptimierung aktiviert sein.

> ***INFO:*** Das System-Flag für die Wegeoptimierung muss bei allen vernetzten OpenScape Business Systemen aktiviert werden!

Die Wegeoptimierung wird ausgeführt:

- Innerhalb des OpenScape Business Netzanteils

- Nach dem Verbindungsaufbau (nicht in der Rufphase!)
- Nach Transferszenarien
- Nach Rufweiterschaltung bzw. Anrufumleitung

Die Wegeoptimierung wird nicht ausgeführt:

- Einer Rufzuschaltung bzw. Gruppenruf
- Bei Konferenzen
- Wenn während der Ausführung der Wegeoptimierung ein anderes Leistungsmerkmal aktiviert wird, wird die Wegeoptimierung abgebrochen.
- Bei inhomogener Vernetzung werden die Fremdsysteme über SIP-Interconnection konfiguriert. In diesem Fall ist, unabhängig von der Konfiguration des Flags, kein Path Replacement möglich (z. B. OpenScape 4000, OpenScape Voice, Externe SIP-Server).

20.5.1 Wie Sie die Wegeoptimierung (Path Replacement) aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **System > System Flags**.

4) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn die Anrufübernahme von Wiederanrufen möglich sein soll, aktivieren Sie das Kontrollkästchen **Wegeoptimierung**.
- Wenn die Anrufübernahme von Wiederanrufen nicht möglich sein soll, deaktivieren Sie das Kontrollkästchen **Wegeoptimierung**.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

20.6 Vernetzungsszenarien

Es gibt mehrere Szenarien, wie OpenScape Business Systeme untereinander und mit anderen Kommunikationssystemen vernetzt werden können.

- Vernetzung von mehreren OpenScape Business X
- Vernetzung von OpenScape Business X und OpenScape Business S (Single Gateway)
- Vernetzung von OpenScape Business X und OpenScape Business S (Multi Gateway)
- Vernetzung von OpenScape Business X und OpenScape 4000/HiPath 4000

- Vernetzung von OpenScape Business X und OpenScape Voice
- Anbindung von externen Anschaltungen an OpenScape Business über SIP-Interconnection
- Offene Nummerierung in OpenScape Business X Netzwerken
- Vernetzung über ISDN
- OpenScape Business Netzverbund mit zentralem ITSP-Amtsanschluss

Gesprächsdaten können nur per Netzknoten, nicht knotenübergreifend abgerufen werden.

20.6.1 Abhängigkeiten und Einschränkungen

Für die möglichen Vernetzungsszenarien gilt es einige Abhängigkeiten und Einschränkungen zu beachten.

Abhängigkeiten und Einschränkungen

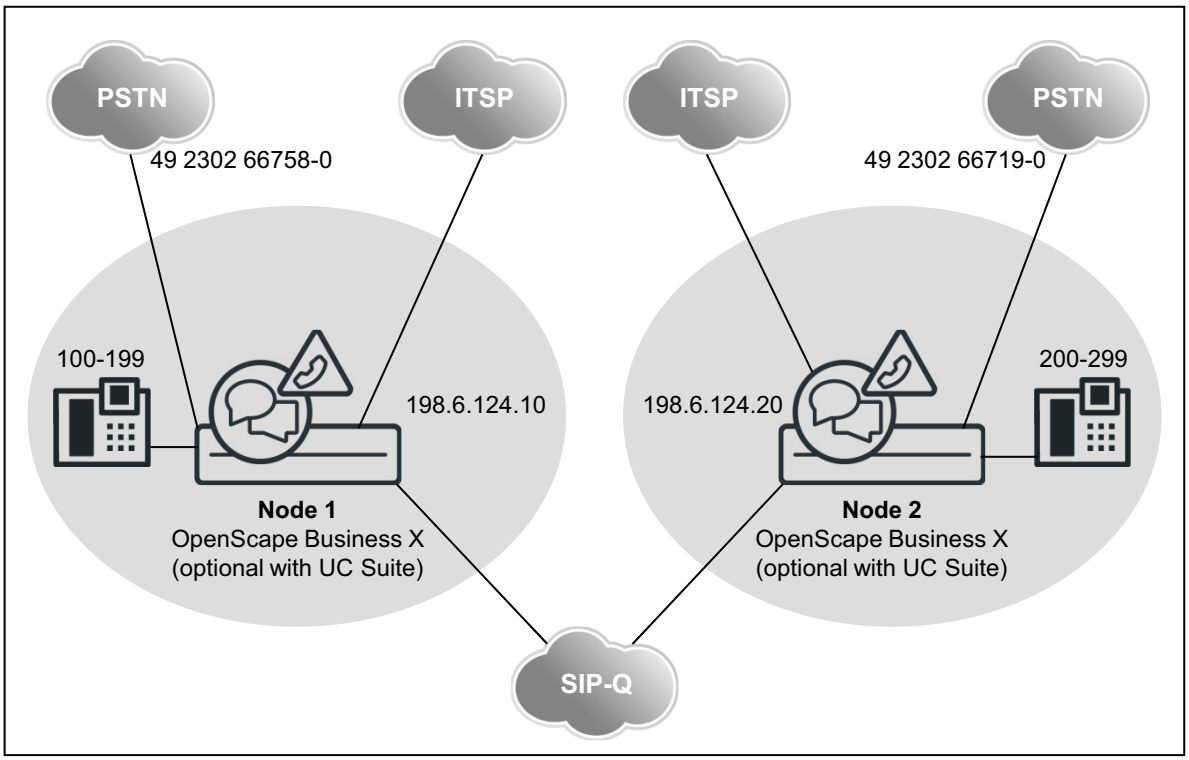
- Für alle Vernetzungsszenarien gilt, dass Server und Clients sich in der gleichen Zeitzone befinden müssen.
- OpenScape Business S Multi-Gateway-Vernetzungen sind nur innerhalb eines Landes (gleiche Zeitzone, gleiche Amtskennzahl) freigegeben.
- Generell wird jeder Netzverbund der OpenScape Business über Wizards konfiguriert. OpenScape Voice und OpenScape 4000/HiPath 4000 werden in der Vernetzung je Knoten über den Expertenmodus konfiguriert.
- Der Presence Manager (DSS Server Funktionalität = netzweite Anzeige von Besetztzuständen an DSS-Tasten + Anrufübernahme) steht in OpenScape Business Netzwerken zur Verfügung.
- SIP-Q Leitungen mit Richtung 16 (letzte Richtung) werden genutzt um homogene OpenScape Business Kommunikationssysteme über den Wizard **Vernetzung-Konfiguration** zu konfigurieren. Externe SIP-Leitungen (SIP-Interconnection) werden für die Vernetzung von OpenScape 4000/ HiPath 4000, OpenScape Voice oder andere Kommunikationssysteme genutzt; die Konfiguration erfolgt über den Experten-Modus.
- Wird das System über den Wizard **Vernetzung-Konfiguration** als Slave oder Master konfiguriert, wird geprüft, ob der Richtung "Networking" Leitungen zugeordnet sind. Wenn nicht, werden der Richtung "Networking" automatisch 16 Leitungen zugeordnet. Wird das System aus dem Netzverbund genommen, bleiben diese Zuordnungen bestehen.
- Hinweise zu den genutzen Company Attendants (UC Smart):
  - Die Funktionalität des Company Attendant (UC Smart) und der Sprachbox sind knotenspezifisch. In jedem Knoten kann nur EIN Voicemail-System zum Einsatz kommen. Generell sind in einem OpenScape Business Netzverbund verschiedenen Voicemail-Systeme erlaubt.
  - Wenn die UC Suite von OpenScape Business genutzt wird, so müssen andere im Netzverbund vorhandene Voicemail-Systeme vom Administrator deaktiviert werden.

– Ein HiPath 3000 Netzverbund mit verschiedenen VoiceMail-Systemen kann 1:1 nach OpenScape Business migriert werden.

INFO: Das vertriebliche Limit kann von diesen Angaben (und den nachfolgenden Angaben in den einzelnen Szenarien) abweichen. Bitte beachten Sie die Hinweise in der Vertriebsinformation.

20.6.2 Szenario 1: Vernetzung von mehreren OpenScape Business X

Bis zu 32 Kommunikationssysteme OpenScape Business X können miteinander vernetzt werden.



Netzwerkdaten

- Geschlossene Nummerierung bei Einsatz der UC Suite
- Geschlossene oder offene Nummerierung bei Einsatz von UC Smart
- Netzweite Sprach- und UC-Funktionalität mit UC-Suite (außer UC Contact Center)
- Netzweite Sprachfunktionalität und lokale UC-Funktionalität mit UC Smart
- Konfiguration über WBM (Wizards) bei geschlossener Nummerierung
- UC Suite Funktionalität basiert auf UC Booster Server oder UC Booster Card
- Bis zu 32 vernetzte Systeme, 1000 User mit UC Smart (UC Smart Funktionen stehen knotenweit zur Verfügung)

- Bis zu 8 vernetzte Systeme, 1000 User mit UC Suite

20.6.3 Szenario 1: Netzweite Leistungsmerkmale

UC Vernetzung	Geschlossene Nummerierung	Offene Nummerierung
Maximale Anzahl Knoten	8 (mit UC Suite) und 32 (ohne UC Suite)	
Maximale Anzahl von Teilnehmern in einem einzelnen Kommunikationssystem	abhängig von OpenScape Business X	
Maximale Anzahl von Teilnehmern im Netz	1000	

UC Vernetzung	Geschlossene Nummerierung	Offene Nummerierung
UC Booster Server	ab 150 Teilnehmer	Wird nicht unterstützt
UC Booster Card	bis 150 Teilnehmer	Wird nicht unterstützt

Administration	Geschlossene Nummerierung	Offene Nummerierung
WBM	Netzweite Administration über Wizards	Netzweite Administration Experten-modus
Manager E	Netzweite Administration für spezielle Aufgaben	Netzweite Administration für spezielle Aufgaben
UC-Suite-Administration (für UC Booster Server und UC Booster Card)	Netzweite Administration über Wizards	Wird nicht unterstützt
Massendatenimport über csv-Dateien (Rufnummern, Durchwahlnummern, Namen)	Separat für jeden Knoten im Netzverbund	

Lizenzierung	Geschlossene Nummerierung	Offene Nummerierung
Neue Lizenzierungsstruktur	Eine Vernetzungs-Lizenz für jeden Knoten erforderlich	

myPortal for Desktop / myPortal for Outlook (UC Suite)	Geschlossene Nummerierung	Offene Nummerierung
	Netzweit mit UC-Funktionalität über UC Booster Server, UC Booster Card oder OpenScape Business S.	Wird nicht unterstützt
Instant Messaging	Netzweit	Wird nicht unterstützt
VoiceMail	Die Teilnehmer nutzer ihr lokales Voice-eMail-System; es gibt keine zentrale VoiceMail für den gesamten Netzverbund.	Wird nicht unterstützt
Anwesenheitsstatus	Netzweit	Wird nicht unterstützt
Besetztanzeige	Netzweit	Wird nicht unterstützt
Internes Verzeichnis / Favoriten	Netzweit	Wird nicht unterstützt

myPortal for Desktop / myPortal for Outlook (UC Suite)	Geschlossene Nummerierung	Offene Nummerierung
Externes Verzeichnis	Lokal über den Import von csv-Dateien	Wird nicht unterstützt
Suche in externen Verzeichnissen anderer Knoten	Nicht möglich	Wird nicht unterstützt
Externes Offline-Verzeichnis (LDAP)	über LDAP	Wird nicht unterstützt

myPortal Smart (UC Smart)	Geschlossene Nummerierung	Offene Nummerierung
	Netzweit	Wird nicht unterstützt
VoiceMail	Die Teilnehmer nutzen ihr lokales VoiceMail-System; es gibt keine zentrale VoiceMail für den gesamten Netzverbund.	Wird nicht unterstützt
Anwesenheitsstatus	Lokal	Wird nicht unterstützt
Besetztanzeige	Lokal	Wird nicht unterstützt
Internes Verzeichnis / Favoriten	Lokal	Wird nicht unterstützt

myAttendant	Geschlossene Nummerierung	Offene Nummerierung
	Mit UC-Funktionalität über UC Booster Server, UC Booster Card oder OpenScape Business S.	Wird nicht unterstützt
Instant Messaging	Netzweit	Wird nicht unterstützt
VoiceMail	Die Teilnehmer nutzen ihr lokales VoiceMail-System; es gibt keine zentrale VoiceMail für den gesamten Netzverbund.	Wird nicht unterstützt
Anwesenheitsstatus	Netzweit	Wird nicht unterstützt
Besetztanzeige	Netzweit	Wird nicht unterstützt
Internes Verzeichnis / Favoriten	Netzweit	Wird nicht unterstützt
Externes Verzeichnis	Lokal über den Import von csv-Dateien	Wird nicht unterstützt
Suche in externen Verzeichnissen anderer Knoten	Nicht möglich	Wird nicht unterstützt
Externes Offline-Verzeichnis (LDAP)	über LDAP	Wird nicht unterstützt
VoiceMail	Die Teilnehmer nutzer ihr lokales VoiceMail-System; es gibt keine zentrale VoiceMail für den gesamten Netzverbund.	Wird nicht unterstützt
VoiceMail-Abfrage für andere Teilnehmer	Lokal, nicht für Teilnehmer in anderen Knoten	Wird nicht unterstützt
Zentraler Vermittlungsplatz	Netzweit	Wird nicht unterstützt

OpenScape Business Attendant	Geschlossene Nummerierung	Offene Nummerierung
	Schnittstelle beschränkt auf 8-stellige Rufnummern	Schnittstelle beschränkt auf 8-stellige Rufnummern
Anwesenheitsstatus	Netzweit über den BLF-Server	Netzweit über den BLF-Server
Besetztanzeige	Netzweit über den BLF-Server	Netzweit über den BLF-Server
Externes Verzeichnis	über LDAP	über LDAP
Zentraler Vermittlungsplatz	Netzweit	Netzweit

Company Auto Attendant (UC Suite)	Geschlossene Nummerierung	Offene Nummerierung
Company AutoAttendant: Nachdem der Auto-Attendant einen Anruf beantwortet hat, muss der Anrufer die Rufnummer wählen mit der er verbunden werden möchte.	ccv-Scripts erlauben es Rufnummern aus dem internen Verzeichnis innerhalb des Netzverbunds zu wählen.	Wird nicht unterstützt
Persönlicher AutoAttendant: Nachdem der AutoAttendant einen Anruf beantwortet hat, muss der Anrufer eine einstellige Ziffer wählen um mit seinem Anrufziel verbunden zu werden.	Jede von einem UC Teilnehmer vorkonfigurierte Rufnummer möglich	Wird nicht unterstützt

Company AutoAttendant (UC Smart)	Geschlossene Nummerierung	Offene Nummerierung
Company AutoAttendant	Lokal	Lokal

myAgent	Geschlossene Nummerierung	Offene Nummerierung
	Mit UC-Funktionalität über UC Booster Server, UC Booster Card Board oder OpenScape Business S. Alle Agenten sind an EINEM Knoten registriert. Eingehend CC-Anrufe über das lokale PSTN, ITSP und SIP-Q-Amtssätze.	Wird nicht unterstützt
VoiceMail (Aufnahme, Message Waiting Indication, Abfrage)	Die Teilnehmer nutzer ihr lokales VoiceMail-System; es gibt keine zentrale VoiceMail für den gesamten Netzverbund	Wird nicht unterstützt
Anwesenheitsstatus	Netzweit	Wird nicht unterstützt
Besetztanzeige	Netzweit	Wird nicht unterstützt
Agentenstatus	Lokal	Wird nicht unterstützt
Internes Verzeichnis / Favoriten	Netzweit	Wird nicht unterstützt
Externes Verzeichnis	Lokal über Import von csv-Dateien	Wird nicht unterstützt
Suche in externen Verzeichnissen anderer Knoten	Nicht möglich	Wird nicht unterstützt
Externes Offline-Verzeichnis (LDAP)	Lokal	Wird nicht unterstützt

myAgent	Geschlossene Nummerierung	Offene Nummerierung
Übergabe eines Anrufs	Lokal	Wird nicht unterstützt
Kundeninformation	Lokal	Wird nicht unterstützt
Reporting	Lokal	Wird nicht unterstützt

Externe Applikationen	Geschlossene Nummerierung	Offene Nummerierung
OpenScape Business TAPI-Applikationen	Siehe *Application Connectivity*	
Externe CSTA-Applikationen		
Application Launcher		
OpenScape Contact Center	Siehe *Multimedia Contact Center*.	

Telefonie	Geschlossene Nummerierung	Offene Nummerierung
SIP-Provider (ITSP)	Lokal	Lokal
PSTN-Provider	Lokal; Netzknoten ohne eigenen PSTN-Provider werden über SIP-Q bzw. das zugehörige Gateway erreicht.	Lokal
Survivability (Ausfallsicherheit im Falle eines Zusammenbruchs des Netzverbundes bzw. der OpenScape Business S)	Nicht relevant in diesem Szenario (keine OpenScape Business S)	Wird nicht unterstützt

Mobility	Geschlossene Nummerierung	Offene Nummerierung
Desksharing	Innerhalb eines Knotens; Netzweit mit DLS	Wird nicht unterstützt
Mobility mit DTMF-Steuerung des Systems	Lokal (wird bei OpenScape Business S nicht unterstützt)	
myPortal for Mobile (UC Suite)	Netzweiter Anwesenheitsstatus und Verzeichnisse (jeder Knoten benötigt dafür entweder UC Booster Card UC Booster Server oder OpenScape Business S)	Wird nicht unterstützt
myPortal for Mobile (UC Smart)	Lokal, nicht für UC Booster Card, UC Booster Server und OpenScape Business S	Wird nicht unterstützt

Sonstige Funktionalitäten	Geschlossene Nummerierung	Offene Nummerierung
Signalling and Payload Encryption SPE	Wird nicht unterstützt bei UC-Verbindungen und Konferenzen	Wird nicht unterstützt bei Konferenzen
DSS-Server	Netzweit (mindestens ein Knoten benötigt dafür entweder UC Booster Card, UC Booster Server oder OpenScape Business S)	Wird nicht unterstützt

20.6.4 Szenario 1: Konfiguration

Die Konfiguration von Szenario 1 (mit geschlossener Nummerierung und UC Suite) zeigt an einem Beispiel, welche Schritte für die Einrichtung einer Vernetzung durchzuführen sind.

Voraussetzungen:

- Es liegt ein Vernetzungsplan vor. Über den Vernetzungsplan ist sichergestellt, dass jede interne Rufnummer im Netzverbund bei verdeckter (geschlossener) Nummerierung nur einmal vergeben ist. Unterschiedliche Rufnummerlängen sind zulässig. Nur Duwa-Rufnummern dürfen mehrfach vorkommen. (z. B. Amtsrufnummer 49 2302 66758 100 und 49 2302 66719 100 haben dieselbe Duwa-Nr. 100).

  INFO: Die Rufnummern müssen ggf. angepasst werden. Eine offene Nummerierung ist nicht implementiert!

- Das IP-Netzwerk ist eingerichtet und alle Knoten können untereinander über Ping erreicht werden
- Alle Knoten sind auf die gleiche Softwareversion hochgerüstet

Knotenübergreifende Rufumleitungen: Bei kommenden Rufen über IP-Trunks, die bereits umgeleitet sind, werden weitere Umleitungen zur Sprachbox nicht ausgeführt. Hintergrund ist, dass ansonsten keine eindeutige Zuordnung zur Sprachbox erfolgen kann

Falls knotenübergreifende Stellvertreterregelungen gewünscht werden, sind diese über Profile der OpenScape Business Teilnehmer oder Rufzuschaltungen einzurichten. Entsprechende knotenübergreifende Anrufe werden in diesem Fall nicht als umgeleitet signalisiert, sondern als Direktruf. Daher werden Rufumleitungen des Stellvertreters zur Sprachbox umgeleitet

Einrichtung der Standortdaten für Knoten 1

Knoten 1		
G.-Standort Land		49
G.-Standort Ortsnetz		2302
G.-Standort Anlage		66758
Internationales Präfix		00
Nationales Präfix		0
Richtungen		
ISDN	AKZ	0
Networking	2. AKZ	0
Richtungsparameter		

Knoten 1		
Richtung	Nr-Typ gehend	RNR-Typ
Networking	Unbekannt	int/Duwa
ISDN	(Keine Änderung des Eintrags)	Duwa

In den Routingtabellen werden automatisch die Rufnummern aller Teilnehmer außerhalb von Knoten 1 eingetragen, und zwar die internen Rufnummern und die DID-Rufnummern, die sich von den jeweiligen internen Rufnummern unterscheiden.

Übersicht der Einträge im LCR für Knoten 1

Wahlplan		Wegetabelle			Wahlregel		
Name	**Gewählte Ziffern**	**Richtung**	**Dediziertes Gateway**	**Gateway ID**	**Wahlregel**	**Verfahren**	**Typ**
Knoten 2 Internat	0C0049230266719-Z	Networking	Erzwungen	2	D49230266719E3A	Corp. Network	International
Knoten 2 NAT	0C0230266719-Z						
Knoten 2 Teiln.	0C66719-Z						
Amt	0CZ	ISDN	No		A	Hauptnetzanbieter	Unknown
Diverse	-Z	Networking	No		A	Corp. Network	Unknown

Einrichtung der Standortdaten für Knoten 2

Knoten 2		
G.-Standort Land		49
G.-Standort Ortsnetz		2302
G.-Standort Anlage		66719
Internationales Präfix		00
Nationales Präfix		0
Richtungen		
ISDN	AKZ	0
Networking	2. AKZ	0
Richtungsparameter		
Richtung	Nr-Typ gehend	RNR-Typ
Networking	Unbekannt	int/Duwa
ISDN	(Keine Änderung des Eintrags)	Duwa

In den Routingtabellen werden automatisch die Rufnummern aller Teilnehmer außerhalb von Knoten 2 eingetragen, und zwar die internen Rufnummern und die DID-Rufnummern, die sich von den jeweiligen internen Rufnummern unterscheiden.

Übersicht der Einträge im LCR für Knoten 2

Wahlplan		Wegetabelle			Wahlregel		
Name	**Gewählte Ziffern**	**Richtung**	**Dediziertes Gateway**	**Gateway ID**	**Wahlregel**	**Verfahren**	**Typ**
Knoten 1 Internat	0C0049230266758-Z	Networking	Erzwungen	1	D49230266758E3A	Corp. Network	International
Knoten 1 NAT	0C0230266758-Z						
Knoten 1 Teiln.	0C66758-Z						
Amt	0CZ	ISDN	No		A	Hauptnetzanbieter	Unknown
Diverse	-Z	Networking	No		A	Corp. Network	Unknown

Vorgehensweise bei der Einrichtung der Vernetzung:

1. Basisinstallation für Knoten 1 (Master) konfigurieren
2. Vernetzung konfigurieren für Knoten 1
3. Basisinstallation für Knoten 2 (Slave) konfigurieren
4. Vernetzung konfigurieren für Knoten 2
5. Vernetzungsfunktion kontrollieren für Master
6. Richtungen und Richtungsparameter überprüfen (Master)
7. Richtungen und Richtungsparameter (Rtg. 16) überprüfen (Master)
8. LCR für die Vernetzung konfigurieren (Master)
9. Richtungen und Richtungsparameter überprüfen (Slave)
10. LCR für die Vernetzung konfigurieren (Slave)

20.6.4.1 Wie Sie die Basisinstallation für Knoten 1 (Master) konfigurieren

Für die Integration in einen Netzwerkverbund müssen die Ländervorwahl und eine Knoten-ID zugewiesen werden. Die internen Rufnummern müssen netzweit eindeutig konfiguriert werden. Die Eingabe der nationalen und lokalen Rufnummern ist wichtig, da diese Rufnummer in der Rtg1 ISDN Amt eingestellt wird und zur Normalisierung als Standortrufnummer verwendet wird.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Grundinstallation**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Basisinstallation** zu starten.

4) Geben Sie im Feld **Ländervorwahl** die Ländervorwahl ein, z. B. 49 für Deutschland.

5) Tragen Sie die **Ortskennzahl** und **Anlagenrufnummer** ein.

6) Aktivieren Sie das Kontrollkästchen **Netzwerk-Integration**.

7) Vergeben Sie im Feld **Knoten-ID** für eine OpenScape Business eine im Netzverbund eindeutige Knoten-ID (eine "**1**" für das Einrichtebeispiel).

8) Klicken Sie auf **Funktion ausführen**. Sie werden zum Fenster **Zentrale Teilnehmer-Funktionen** geführt.

9) Da in einem Netzwerk alle internen Rufnummern eindeutig sein müssen, sind die Standard-Rufnummern zu löschen. Aktivieren Sie dazu das Optionsfeld **Alle Rufnummern löschen**.

10) Aktivieren Sie das Kontrollkästchen **Alle Rufnummern löschen** und klicken Sie auf **OK & Weiter**. Sie werden zum Fenster **Vorkonfigurierte Rufnummern ändern** geführt.

> ***INFO:*** Die Funktionskennzahlen müssen im Netzwerkverbund eindeutig sein. Doppelte Rufnummern sind nicht zulässig!

11) Passen Sie die vorkonfigurierten Rufnummern an die Rufnummern im Netzwerk an und klicken Sie auf **OK & Weiter**. Die Rufnummern können Sie entweder manuell über den Wizard anpassen oder Sie importieren eine CSV-Datei mit den entsprechend vorbereiteten Rufnummern.

12) Konfigurieren Sie jetzt die IP-Clients.

13) Ändern Sie die Einstellungen für eine MeetMe-Konferenz. Sie müssen eine eindeutige Kennzahl im Netzwerkverbund eingeben.

14) Konfigurieren Sie jetzt den E-Mail-Versand.

15) Klicken Sie auf **Beenden**.

20.6.4.2 Wie Sie die Vernetzung für Knoten 1 (Master) konfigurieren

Im nächsten Schritt wird der Wizard für die Vernetzung konfiguriert.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Grundinstallation**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Vernetzung-Konfiguration** zu starten.

4) Wählen Sie die Einstellung **Netzwerk mit OSBiz X / OSBiz S**.

5) Definieren Sie den Knotentyp (**Master**).

6) Geben Sie unter **Node-ID** die entsprechenden Knotennummern der zugehörigen OpenScape Business Systeme ein (im Einrichtebeispiel die des Slaves mit der Node-ID 2).

7) Geben Sie unter **IP-Adresse** die IP-Adressen der zugehörigen OpenScape Business Systeme ein (im Einrichtebeispiel die des Slaves mit der Node-ID 2).

8) Geben Sie unter **Name** den entsprechenden Typ der Unteranlage ein.

9) Aktivieren Sie ggf. das Kontrollkästchen **Verschlüsselung**.

INFO: Die Verschlüsselung basiert auf SPE und gilt nicht für die Applikationen!

HINWEIS: Durch die Aktivierung des Kontrollkästchens ist noch keine Verschlüsselung konfiguriert. Siehe *Signaling and Payload Encryption SPE*.

10) Klicken Sie auf **Beenden**.

20.6.4.3 Wie Sie die Basisinstallation für Knoten 2 (Slave) konfigurieren

Für die Integration in einen Netzwerkverbund müssen die Ländervorwahl und eine Knoten-ID zugewiesen werden. Die internen Rufnummern müssen netzweit eindeutig konfiguriert werden. Die Eingabe der nationalen und lokalen Rufnummern ist wichtig, da diese Rufnummer in der Rtg1 ISDN Amt eingestellt wird und zur Normalisierung als Standortrufnummer verwendet wird.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Basisinstallation**.

3) Geben Sie im Feld **Ländervorwahl** die Ländervorwahl ein, z. B. 49 für Deutschland.

4) Tragen Sie die **Ortskennzahl** und **Anlagenrufnummer** ein.

5) Aktivieren Sie das Kontrollkästchen **Netzwerk-Integration**.

6) Vergeben Sie im Feld **Knoten-ID** für OpenScape Business S eine im Netzverbund eindeutige Knoten-ID (eine "**2**" für das Einrichtebeispiel).

7) Klicken Sie auf **Funktion ausführen**. Sie werden zum Fenster **Zentrale Teilnehmer-Funktionen** geführt.

8) Da in einem Netzwerk alle internen Rufnummern eindeutig sein müssen, sind die Standard-Rufnummern zu löschen. Aktivieren Sie dazu das Optionsfeld **Alle Rufnummern löschen**.

9) Aktivieren Sie das Kontrollkästchen **Alle Rufnummern löschen** und klicken Sie auf **OK & Weiter**. Sie werden zum Fenster **Vorkonfigurierte Rufnummern ändern** geführt.

> ***INFO:*** Die Funktionskennzahlen müssen im Netzwerkverbund eindeutig sein. Doppelte Rufnummern sind nicht zulässig!

10) Passen Sie die vorkonfigurierten Rufnummern an die Rufnummern im Netzwerk an und klicken Sie auf **OK & Weiter**. Die Rufnummern können Sie entweder manuell über den Wizard anpassen oder Sie importieren eine CSV-Datei mit den entsprechend vorbereiteten Rufnummern.

11) Konfigurieren Sie jetzt die IP-Clients.

12) Ändern Sie die Einstellungen für eine MeetMe-Konferenz. Sie müssen eine eindeutige Kennzahl im Netzwerkverbund eingeben.

13) Konfigurieren Sie jetzt den E-Mail-Versand.

14) Klicken Sie auf **Beenden**.

20.6.4.4 Wie Sie die Vernetzung für Knoten 2 (Slave) konfigurieren

Im nächsten Schritt wird der Wizard für die Vernetzung konfiguriert.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Grundinstallation**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Vernetzung-Konfiguration** zu starten.

4) Wählen Sie die Einstellung **Netzwerk mit OSBiz X / OSBiz S**.

5) Aktivieren Sie unter **Knotentyp** das Kästchen **Dieses System ist ein SLAVE-Knoten**.

6) Geben Sie unter **IP-Adresse** die IP-Adresse des Masters ein.

> ***INFO:*** Nach dem Klicken von **OK & Weiter** kann diese Aktion nicht mehr rückgängiggemacht werden!

7) Der **Registrierungsstatus** wird mit **Status erfolgreich** angezeigt (oder mit entsprechender Fehlermeldung). Damit ist der Wizard abgeschlossen.

8) Klicken Sie auf **Beenden**.

20.6.4.5 Wie Sie die Vernetzungsfunktion für den Master kontrollieren

Sie können den Status der Vernetzung generell und die einzelnen Rufnummern kontrollieren.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Netzwerk**.

2) In der Statuszeile sehen Sie den **Synchronisationsstatus** für das Netzwerk. Grün bedeutet, dass die Vernetzung keine Probleme hat, Rot bedeutet Probleme im Netzwerk.

3) Markieren Sie im Fenster **Netzwerk** die Registerkarte **Knoten-Sicht** und es werden alle verfügbaren Knoten mit **Knoten ID**, **Name**, **System Typ**, **Server Adresse**, **Registrierungsstatus** und **Verfügbarkeitsstatus** angezeigt.

4) Markieren sie im Fenster **Netzwerk** die Registerkarte **Rufnummern** und es öffnet sich ein Fenster mit allen Angaben zu:

Rufnummer
DuWa
Name
Port Typ
Knoten

20.6.4.6 Wie Sie Richtungen und Richtungsparameter konfigurieren (ISDN-Amt für den Master)

Mit folgenden Schritten konfigurieren Sie die Richtungen für die Vernetzung des Masters.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Leitungen/Vernetzung**.
3) Klicken Sie im Menübaum auf **Richtung**.
4) Geben Sie im Fenster **Richtung ändern** im Feld **Richtungsname** einen Namen `Rtg. 1` für die Amtsrichtung ein.
5) Geben Sie unter **Richtungskennzahl** die `0` ein.
6) Geben Sie unter **Anlagenrufnummer-kommend** im Feld **Ländervorwahl** die `49` ein.
7) Geben Sie unter **Anlagenrufnummer-kommend** im Feld **Ortsnetzkennzahl** die `2302` ein.
8) Geben Sie unter **Anlagenrufnummer-kommend** im Feld **Anlagenrufnummer** die `66758` ein.
9) Markieren Sie das Kontrollkästchen unter **Anlagenrufnummer-kommend** im Feld **Standort-Nummer**.
10) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

20.6.4.7 Wie Sie Richtungen und Richtungsparameter (Rtg. 16) konfigurieren (Master)

Für die Richtung 16 (Networking) ist es für Master und Slave zwingend erforderlich, den Eintrag für das 2. AKZ auszufüllen. Richtung 16 ist die Standard-Richtung für die Vernetzung bei OpenScape Business.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Leitungen/Vernetzung**.
3) Klicken Sie im Menübaum auf die letzte **Richtung** (**Rtg. 16**).
4) Geben Sie im Fenster **Richtung ändern** im Feld **Richtungsname** einen Namen `Networking` für die Vernetzungsrichtung ein.
5) Geben Sie unter **Richtungskennzahl** nichts ein.
6) Geben Sie unter **Amtskennziffer (2. AKZ)** die 0 ein.
7) Die Defaulte-Einstellungen für die Richtungsparameter (Nr.-Typ, gehen, Rufnummer Typ) können übernommen werden.
8) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

20.6.4.8 Wie Sie LCR für die Vernetzung konfigurieren (Master)

Im LCR Wahlplan sind die Default-Einträge im Index 32, 33 und 34 um weitere Einträge für die Wahl von Rufnummern im Format "International, National und Teilnehmer" zum Knoten 2 zu ergänzen. "International" und "National" werden immer benötigt, "Teilnehmer" nur für Partnerknoten, die sich im gleichen Ortsnetz befinden. Diese Angaben werden für die Wahl aus Applikationen (z. B. myPortal for Desktop) verwendet.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > LCR**.

3) Klicken Sie im Menübaum auf **Wahlplan**.

4) Geben Sie folgende Werte auf freien Plätzen (hier 35 bis 37) nach den Standardwerten ein:

Wahlplan	Name	Gewählte Ziffern	Wegetabelle
32	Standard	88CZ	1
33	IP-Network	-Z	13
34	COInternat	0C0049-Z	14
35	Knoten 2 Inter	0C0049230266719-Z	16
36	Knoten 2 Nat	0C0230266719-Z	16
37	Knoten 2 Teiln.	0C66719-Z	16

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

6) Klicken Sie im Menübaum auf die zugehörige **Wahlregel** für Knoten 2.

a) Geben Sie unter **Regelname** den Eintrag **Knoten 2** ein.

b) Geben Sie unter **Wahlregelformat** den Eintrag **D49230266719E3A** ein.

c) Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus.

d) Wählen Sie unter **Type** den Eintrag **Ländervorwahl** aus.

e) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

7) Klicken Sie im Menübaum auf **Wegetabelle**.

8) Klicken Sie auf die Wegetabelle 16.

a) Wählen Sie unter **Richtung** den Eintrag **Networking** aus.

b) Wählen Sie unter **Wahlregel** den Eintrag **Knoten 2** aus.

c) Wählen Sie unter **Min. Ber.** den Eintrag **15** aus.

d) Wählen Sie unter **Warnung** den Eintrag **Keine** aus.

e) Wählen Sie unter **Dediziertes Gateway** den Eintrag **Erzwungen** aus.

f) Wählen Sie unter **GW Knoten-ID** den Eintrag **2** aus.

g) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

20.6.4.9 Wie Sie die Richtung und Richtungsparameter konfigurieren (Slave)

Mit folgenden Schritten können Sie die Richtung und Richtungsparamter für die Vernetzung des Slaves konfigurieren.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Leitungen/Vernetzung**.

3) Klicken Sie im Menübaum auf **Richtung**.

4) Geben Sie im Fenster **Richtung ändern** im Feld **Richtungsname** einen Namen `Rtg. 1` für die Vernetzungsrichtung ein.

5) Geben Sie unter **Richtungskennzahl** die `0` ein.

6) Geben Sie unter **Anlagenrufnummer-kommend** im Feld **Ländervorwahl** die `49` ein.

7) Geben Sie unter **Anlagenrufnummer-kommend** im Feld **Ortsnetzkennzahl** die `2302` ein.

8) Geben Sie unter **Anlagenrufnummer-kommend** im Feld **Anlagenrufnummer** die `66719` ein.

9) Markieren Sie das Kontrollkästchen unter **Anlagenrufnummer-kommend** im Feld **Standort-Nummer**.

10) Die Default-Einstellungen für die Richtungsparameter (Nr.-Typ, gehen, Rufnummer Typ) können übernommen werden.

11) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

20.6.4.10 Wie Sie LCR für die Vernetzung konfigurieren (Slave)

Im LCR Wahlplan sind die Default-Einträge im Index 32, 33, 34 and 35 um weitere Einträge für die Wahl von Rufnummern im Format "International, National und Teilnehmer" zum Knoten 2 zu ergänzen. "International" und "National" werden immer benötigt, "Teilnehmer" nur für Partnerknoten, die sich im gleichen Ortsnetz befinden. Diese Angaben werden für die Wahl aus Applikationen (z. B. myPortal for Desktop) verwendet.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > LCR**.

3) Klicken Sie im Menübaum auf **Wahlplan**.

4) Geben Sie folgende Werte auf freien Plätzen (hier 35 bis 37) nach den Standardwerten ein:

Wahlplan	Name	Gewählte Ziffern	Wegetabelle
32	Standard	88CZ	1
33	IP-Network	-Z	13
34	COInternat	0C0049-Z	14
36	Knoten 1 Inter	0C0049230266758-Z	16
37	Knoten 1 Nat	0C00230266758-Z	16
38	Knoten 1 Teiln.	0C66758-Z	16

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

6) Klicken Sie im Menübaum auf **Wahlregel** für **Knoten 2**.

a) Geben Sie unter **Regelname** den Eintrag **Knoten 1** ein.

b) Geben Sie unter **Wahlregelformat** den Eintrag **D49230266758E3A** ein.

c) Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus.

d) Wählen Sie unter **Type** den Eintrag **Ländervorwahl** aus.

e) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

7) Klicken Sie auf die Wegetabelle 16.

a) Wählen Sie unter **Richtung** den Eintrag **Networking** aus.

b) Wählen Sie unter **Wahlregel** den Eintrag **Knoten 1** aus.

c) Wählen Sie unter **Min. Ber.** den Eintrag **15** aus.

d) Wählen Sie unter **Warnung** den Eintrag **Keine** aus.

e) Wählen Sie unter **Dediziertes Gateway** den Eintrag **Erzwungen** aus.

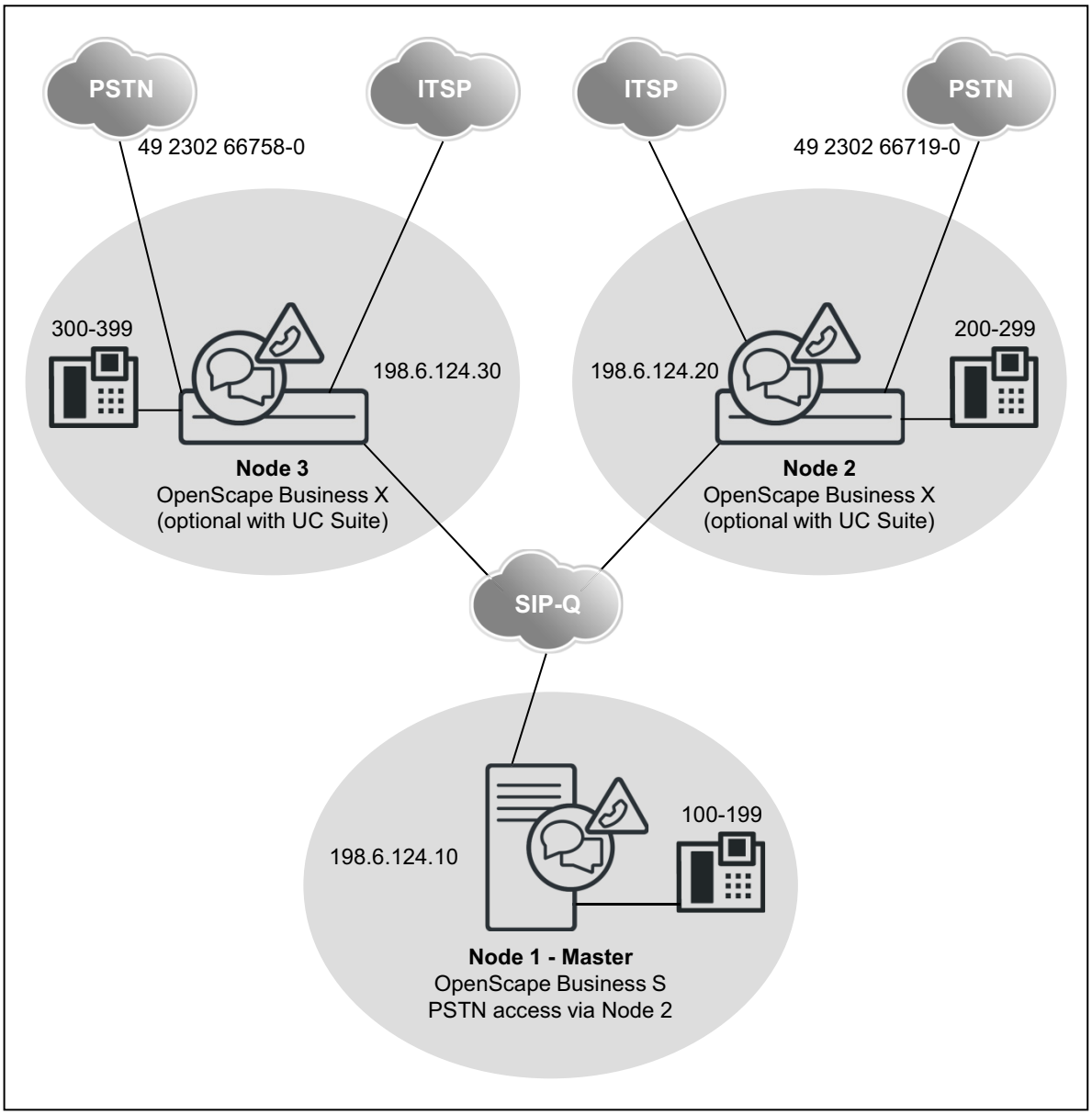
f) Wählen Sie unter **GW Knoten-ID** den Eintrag **2** aus.

g) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

8) Klicken Sie im Menübaum auf **Wegetabelle**.

20.6.5 Szenario 2: Vernetzung von OpenScape Business X mit OpenScape Business S (Single Gateway)

Bis zu 32 Kommunikationssysteme OpenScape Business X/S können miteinander vernetzt werden. Dabei sind mehrere OpenScape Business S in einem Netzverbund erlaubt. Single Gateway bedeutet, dass alle an OpenScape Business S registrierten IP-Teilnehmer nur EIN Gateway zum PSTN verwenden.



Netzwerkdaten

- Geschlossene Nummerierung

- Netzweite Sprach- und UC-Funktionalität mit UC Suite Konfiguration über WBM (Wizards)
- Die UC-Funktionalität ist entweder über UC Booster Server oder über UC Booster Card realisiert
- Die UC-Funktionalität der OpenScape Business S ist integriert
- Es sind mehrere OpenScape Business S im Netzverbund erlaubt.
- Bis zu 32 vernetzte Systeme, 1000 User mit UC Smart (UC Smart Funktionen stehen knotenweit zur Verfügung)
- Bis zu 8 vernetzte Systeme, 1000 User mit UC Suite

20.6.6 Szenario 2: Netzweite Leistungsmerkmale

UC Vernetzung	Geschlossene Nummerierung	Offene Nummerierung
Maximale Anzahl Knoten	8 (mit UC Suite) und 32 (ohne UC Suite)	
Maximale Anzahl von Teilnehmern in einem einzelnen Kommunikationssystem	abhängig von OpenScape Business X	
Maximale Anzahl von Teilnehmern im Netz	1000	

UC Vernetzung	Geschlossene Nummerierung	Offene Nummerierung
UC Booster Server	ab 150 Teilnehmer	Wird nicht unterstützt
UC Booster Card	bis 150 Teilnehmer	Wird nicht unterstützt

Administration	Geschlossene Nummerierung	Offene Nummerierung
WBM	Netzweite Administration über Wizards	Wird nicht unterstützt
Manager E	Netzweite Administration für spezielle Aufgaben	Wird nicht unterstützt
UC-Suite-Administration (für UC Booster Server und UC Booster Card)	Netzweite Administration über Wizards	Wird nicht unterstützt
Massendatenimport über csv-Dateien (Rufnummern, Durchwahlnummern, Namen)	Separat für jeden Knoten im Netzverbund	Wird nicht unterstützt

Lizenzierung	Geschlossene Nummerierung	Offene Nummerierung
Neue Lizenzierungsstruktur	Eine Vernetzungs-Lizenz für jeden Knoten erforderlich	Wird nicht unterstützt

myPortal for Desktop / myPortal for Outlook (UC Suite)	Geschlossene Nummerierung	Offene Nummerierung
	Netzweit mit UC-Funktionalität über UC Booster Server, UC Booster Card oder OpenScape Business S	Wird nicht unterstützt
Instant Messaging	Netzweit	Wird nicht unterstützt
VoiceMail	Die Teilnehmer nutzer ihr lokales VoiceMail-System; es gibt keine zentrale VoiceMail für den gesamten Netzverbund.	Wird nicht unterstützt
Anwesenheitsstatus	Netzweit	Wird nicht unterstützt
Besetztanzeige	Netzweit	Wird nicht unterstützt
Internes Verzeichnis / Favoriten	Netzweit	Wird nicht unterstützt
Externes Verzeichnis	Lokal über den Import von csv-Dateien	Wird nicht unterstützt
Suche in externen Verzeichnissen anderer Knoten	Nicht möglich	Wird nicht unterstützt
Externes Offline-Verzeichnis (LDAP)	über LDAP	Wird nicht unterstützt

myPortal Smart (UC Smart)	Geschlossene Nummerierung	Offene Nummerierung
	Netzweit	Wird nicht unterstützt
VoiceMail	Die Teilnehmer nutzen ihr lokales VoiceMail-System; es gibt keine zentrale VoiceMail für den gesamten Netzverbund.	Wird nicht unterstützt
Anwesenheitsstatus	Lokal	Wird nicht unterstützt
Besetztanzeige	Lokal	Wird nicht unterstützt
Internes Verzeichnis / Favoriten	Lokal	Wird nicht unterstützt

myAttendant	Geschlossene Nummerierung	Offene Nummerierung
	Mit UC-Funktionalität über UC Booster Server, UC Booster Card oder OpenScape Business S	Wird nicht unterstützt
Instant Messaging	Netzweit	Wird nicht unterstützt
VoiceMail	Die Teilnehmer nutzen ihr lokales VoiceMail-System; es gibt keine zentrale VoiceMail für den gesamten Netzverbund.	Wird nicht unterstützt
Anwesenheitsstatus	Netzweit	Wird nicht unterstützt
Besetztanzeige	Netzweit	Wird nicht unterstützt
Internes Verzeichnis / Favoriten	Netzweit	Wird nicht unterstützt

myAttendant	Geschlossene Nummerierung	Offene Nummerierung
Externes Verzeichnis	Lokal über den Import von csv-Dateien	Wird nicht unterstützt
Suche in externen Verzeichnissen anderer Knoten	Nicht möglich	Wird nicht unterstützt
Externes Offline-Verzeichnis (LDAP)	über LDAP	Wird nicht unterstützt
VoiceMail	Die Teilnehmer nutzer ihr lokales VoiceMail-System; es gibt keine zentrale VoiceMail für den gesamten Netzverbund.	Wird nicht unterstützt
VoiceMail-Abfrage für andere Teilnehmer	Lokal, nicht für Teilnehmer in anderen Knoten	Wird nicht unterstützt
Zentraler Vermittlungsplatz	Netzweit	Wird nicht unterstützt

OpenScape Business Attendant	Geschlossene Nummerierung	Offene Nummerierung
	Schnittstelle beschränkt auf 8-stellige Rufnummern	Wird nicht unterstützt
Anwesenheitsstatus	Netzweit über den BLF-Server	Wird nicht unterstützt
Besetztanzeige	Netzweit über den BLF-Server	Wird nicht unterstützt
Externes Verzeichnis	über LDAP	Wird nicht unterstützt
Zentraler Vermittlungsplatz	Netzweit	Wird nicht unterstützt

Company AutoAttendant (UC Suite)	Geschlossene Nummerierung	Offene Nummerierung
Company AutoAttendant: Nachdem der Auto-Attendant einen Anruf beantwortet hat, muss der Anrufer die Rufnummer wählen mit der er verbunden werden möchte.	ccv-Scripts erlauben es Rufnummern aus dem internen Verzeichnis innerhalb des Netzverbunds zu wählen.	Wird nicht unterstützt
Persönlicher AutoAttendant: Nachdem der AutoAttendant einen Anruf beantwortet hat, muss der Anrufer eine einstellige Ziffer wählen um mit seinem Anrufziel verbunden zu werden.	Jede von einem UC Teilnehmer vorkonfigurierte Rufnummer möglich	Wird nicht unterstützt

Company AutoAttendant (UCSmart)	Geschlossene Nummerierung	Offene Nummerierung
Company AutoAttendant	Lokal	Lokal

myAgent	Geschlossene Nummerierung	Offene Nummerierung
	Mit UC-Funktionalität über UC Booster Server, UC Booster Card oder OpenScape Business S. Alle Agenten sind an EINEM Knoten registriert. Eingehend CC-Anrufe über das lokale PSTN, ITSP und SIP-Q-Amtssätze.	Wird nicht unterstützt
VoiceMail (Aufnahme, Message Waiting Indication, Abfrage)	Die Teilnehmer nutzer ihr lokales VoiceMail-System; es gibt keine zentrale VoiceMail für den gesamten Netzverbund	Wird nicht unterstützt
Anwesenheitsstatus	Netzweit	Wird nicht unterstützt
Besetztanzeige	Netzweit	Wird nicht unterstützt
Agentenstatus	Lokal	Wird nicht unterstützt
Internes Verzeichnis / Favoriten	Netzweit	Wird nicht unterstützt
Externes Verzeichnis	Lokal über Import von csv-Dateien	Wird nicht unterstützt
Suche in externen Verzeichnissen anderer Knoten	Nicht möglich	Wird nicht unterstützt
Externes Offline-Verzeichnis (LDAP)	Lokal	Wird nicht unterstützt
Übergabe eines Anrufs	Lokal	Wird nicht unterstützt
Kundeninformation	Lokal	Wird nicht unterstützt
Reporting	Lokal	Wird nicht unterstützt

Externe Applikationen	Geschlossene Nummerierung	Offene Nummerierung
OpenScape Business TAPI-Applikationen	Siehe *Application Connectivity*	
Externe CSTA-Applikationen		
Application Launcher		
OpenScape Contact Center	Siehe *Multimedia Contact Center*.	

Telefonie	Geschlossene Nummerierung	Offene Nummerierung
SIP-Provider (ITSP)	Lokal	Lokal
PSTN-Provider	Lokal; Netzknoten ohne eigenen PSTN-Provider werden über SIP-Q bzw. das zugehörige Gateway erreicht.	Lokal
Survivability (Ausfallsicherheit im Falle eines Zusammenbruchs des Netzverbundes bzw. der OpenScape Business S)	Lokal	Lokal

Mobility	Geschlossene Nummerierung	Offene Nummerierung
Desksharing	Innerhalb eines Knotens; Netzweit mit DLS	Wird nicht unterstützt
Mobility mit DTMF-Steuerung des Systems	Lokal (wird bei OpenScape Business S nicht unterstützt)	
myPortal for Mobile (UC Suite)	Netzweiter Anwesenheitsstatus und Verzeichnisse (jeder Knoten benötigt dafür entweder UC Booster Server, UC Booster Card , oder OpenScape Business S)	Wird nicht unterstützt
myPortal for Mobile (UC Smart)	Lokal, nicht für UC Booster Server, UC Booster Card, und OpenScape Business S	Wird nicht unterstützt

Sonstige Funktionalitäten	Geschlossene Nummerierung	Offene Nummerierung
Signalling and Payload Encryption SPE	Wird nicht unterstützt bei UC-Verbindungen und Konferenzen	Wird nicht unterstützt bei Konferenzen
DSS-Server	Netzweit	Wird nicht unterstützt

20.6.7 Szenario 2: Konfiguration

Die Konfiguration von Szenario 2 (mit geschlossener Nummerierung und UC Suite) zeigt an einem Beispiel, welche Schritte für die Einrichtung einer Vernetzung durchzuführen sind.

Voraussetzungen:

- Es liegt ein Vernetzungsplan vor. Über den Vernetzungsplan ist sichergestellt, dass jede interne Rufnummer im Netzverbund bei verdeckter Nummerierung nur einmal vergeben ist. Unterschiedliche Rufnummernlängen sind zulässig. Nur Duwa-Rufnummern dürfen mehrfach vorkommen. (z. B. Amtsrufnummer 49 2302 66758 100 und 49 2302 66719 100 haben die selbe Duwa-Nr. 100).
- Das IP-Netzwerk ist eingerichtet und alle Knoten können untereinander über Ping erreicht werden

Knotenübergreifende Rufumleitungen: Bei kommenden Rufen über IP-Trunks, die bereits umgeleitet sind, werden weitere Umleitungen zur Sprachbox nicht ausgeführt. Hintergrund ist, dass ansonsten keine eindeutige Zuordnung zur Sprachbox erfolgen kann

Falls knotenübergreifende Stellvertreterregelungen gewünscht werden, sind diese über Profile der OpenScape Business Teilnehmer oder Rufzuschaltungen einzurichten. Entsprechende knotenübergreifende Anrufe werden in diesem Fall nicht als umgeleitet signalisiert, sondern als Direktruf. Daher werden Rufumleitungen des Stellvertreters zur Sprachbox umgeleitet.

Netzverbund in der Activation Period

> ***INFO:*** In einem Netzverbund, in dem die Activation Period verwendet wird, muss immer der CLA von OpenScape Business S als zentraler CLA verwendet werden!

Aufgrund unterschiedlichen Mengen-Obergrenzen werden zwei verschiedene Activation-Period-Dateien für OpenScape Business und OpenScape Business S benötigt. Die Activation-Period-Datei für OpenScape Business S enthält für Netzwerkszenarien zusätzlich zur S-Basis auch die Basis für OpenScape Business.

Wenn in diesem Szenario OpenScape Business eine Lizenzanfrage innerhalb der Activation Period an einen CLA der OpenScape Business S richtet, werden die Grenzwerte von OpenScape Business S verwendet.

Würde dagegen der CLA der OpenScape Business verwendet, so würde eine anfragende OpenScape Business S KEINE Activation Period erhalten, da in dieser Datei keine Basis für OpenScape Business S enthalten ist.

Einrichtung der Standortdaten für Knoten 1 OpenScape Business S

Knoten 1		
G.-Standort Land		49
G.-Standort Ortsnetz		2302
G.-Standort Anlage		66719
Internationales Prefix		00
Nationales Prefix		0
Richtungen		
Rtg. 1	AKZ	0
Networking	2. AKZ	0
Richtungsparameter		
Richtung	Nr-Typ gehend	RNR-Typ
Networking	Unbekannt	int/Duwa
ISDN	(Keine Änderung des Eintrags)	Duwa

In den Routingtabellen werden automatisch die Rufnummern aller Teilnehmer außerhalb von Knoten 1 eingetragen, und zwar die internen Rufnummern und die DID-Rufnummern, die sich von den jeweiligen internen Rufnummern unterscheiden.

Übersicht der Einträge im LCR für Knoten 1

Wahlplan		Wegetabelle			Wahlregel		
Name	**Gewählte Ziffern**	**Richtung**	**Dediziertes Gateway**	**Gateway ID**	**Wahlregel**	**Verfahren**	**Typ**
Knoten 2 Internat	0C0049230266719-2Z	Networking	Erzwungen	2	D49230266719E3A	Corp. Network	International
Knoten 2 NAT	0C0230266719-2Z						
Knoten 2 Teiln.	0C66719-2Z						
Knoten 3 Internat	0C0049230266758-3Z	Networking	Erzwungen	3	D49230266758E3A	Corp. Network	International
Knoten 3 NAT	0C0230266758-3Z						
Knoten 3 Teiln.	0C66758-3Z						
Amt	0CZ	Networking	Erzwungen	2	E1A	Hauptnetzanbieter	Unknown
Diverse	-Z	Networking	No		A	Corp. Network	Unknown

Einrichtung der Standortdaten für Knoten 2 OpenScape Business

Knoten 2		
G.-Standort Land		49
G.-Standort Ortsnetz		2302
G.-Standort Anlage		66719
Internationales Prefix		00
Nationales Prefix		0
Richtungen		
ISDN	AKZ	0
Networking	2. AKZ	0
Richtungsparameter		
Richtung	Nr-Typ gehend	RNR-Typ
Networking	Unbekannt	int/Duwa
ISDN	(Keine Änderung des Eintrags)	Duwa

In den Routingtabellen werden automatisch die Rufnummern aller Teilnehmer außerhalb von Knoten 2 eingetragen, und zwar die internen Rufnummern und die DID-Rufnummern, die sich von den jeweiligen internen Rufnummern unterscheiden.

Übersicht der Einträge im LCR für Knoten 2

Wahlplan		Wegetabelle			Wahlregel		
Name	**Gewählte Ziffern**	**Richtung**	**Dediziertes Gateway**	**Gateway ID**	**Wahlregel**	**Verfahren**	**Typ**
Knoten 1 Internat	0C0049230266719-1Z	Networking	Erzwungen	1	D49230266719E3A	Corp. Network	International
Knoten 1 NAT	0C0230266719-1Z						
Knoten 1 Teiln.	0C66719-1Z						
Knoten 3 Internat	0C0049230266758-3Z	Networking	Erzwungen	3	D49230266758E3A	Corp. Network	International
Knoten 3 NAT	0C0230266758-3Z						
Knoten 3 Teiln.	0C66758-3Z						
Amt	0CZ	ISDN	No		A	Hauptnetzanbieter	Unknown
Diverse	-Z	Networking	No		A	Corp. Network	Unknown

Einrichtung der Standortdaten für Knoten 3 OpenScape Business

Knoten 3		
G.-Standort Land		49
G.-Standort Ortsnetz		2302
G.-Standort Anlage		66758
Internationales Prefix		00
Nationales Prefix		0
Richtungen		
ISDN	AKZ	0
Networking	2. AKZ	0
Richtungsparameter		
Richtung	Nr-Typ gehend	RNR-Typ
Networking	Unbekannt	int/Duwa
ISDN	(Keine Änderung des Eintrags)	Duwa

In den Routingtabellen werden automatisch die Rufnummern aller Teilnehmer außerhalb von Knoten 3 eingetragen, und zwar die internen Rufnummern und die DID-Rufnummern, die sich von den jeweiligen internen Rufnummern unterscheiden.

Übersicht der Einträge im LCR für Knoten 3

Wahlplan		Wegetabelle			Wahlregel		
Name	**Gewählte Ziffern**	**Richtung**	**Dediziertes Gateway**	**Gateway ID**	**Wahlregel**	**Verfahren**	**Typ**
Knoten 1 Internat	0C0049230266719-1Z	Networking	Erzwungen	1	D49230266719E3A	Corp. Network	International
Knoten 1 NAT	0C0230266719-1Z						
Knoten 1 Teiln.	0C66719-1Z						
Knoten 2 Internat	0C0049230266719-2Z	Networking	Erzwungen	2	D49230266719E3A	Corp. Network	International
Knoten 2 NAT	0C0230266719-2Z						
Knoten 2 Teiln.	0C66719-2Z						
Amt	0CZ	ISDN	No		A	Hauptnetzanbieter	Unknown
Diverse	-Z	Networking	No		A	Corp. Network	Unknown

Vorgehensweise bei der Einrichtung der Vernetzung:

1. Basisinstallation für Knoten 1 (Master) konfigurieren
2. Vernetzung konfigurieren für Knoten 1
3. Basisinstallation für Knoten 2 (Slave) konfigurieren
4. Vernetzung konfigurieren für Knoten 2
5. Basisinstallation für Knoten 3 (Slave) konfigurieren
6. Vernetzung konfigurieren für Knoten 3 (Slave)
7. Vernetzungsfunktion kontrollieren für Master
8. LCR für die Vernetzung konfigurieren (Knoten 1, Master)
9. LCR für die Vernetzung konfigurieren (Knoten 2)
10. Richtungen und Richtungsparameter konfigurieren (Knoten 3)
11. Richtungen und Richtungsparameter (Rtg. 16) konfigurieren (Knoten 3)
12. LCR für die Vernetzung konfigurieren (Knoten 3)

20.6.7.1 Wie Sie die Basisinstallation für Knoten 1 (Master) konfigurieren

Für die Integration in einen Netzwerkverbund müssen die Ländervorwahl und eine Knoten-ID zugewiesen werden. Die internen Rufnummern müssen netzweit eindeutig konfiguriert werden. Die Eingabe der nationalen und lokalen Rufnummern ist wichtig, da diese Rufnummer in der Rtg1 ISDN Amt eingestellt wird und zur Normalisierung als Standortrufnummer verwendet wird.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Basisinstallation**.

3) Geben Sie im Feld **Ländervorwahl** die Ländervorwahl ein, z. B. 49 für Deutschland.

4) Tragen Sie die **Ortskennzahl** und **Anlagenrufnummer** ein.

5) Aktivieren Sie das Kontrollkästchen **Netzwerk-Integration**.

6) Vergeben Sie im Feld **Knoten-ID** für OpenScape Business S eine im Netzverbund eindeutige Knoten-ID. Die Knoten-ID muss zwischen "**1**" und "**100**" sein (eine "**1**" für das Einrichtebeispiel wählen).

7) Klicken Sie auf **Funktion ausführen**. Sie werden zum Fenster **Zentrale Teilnehmer-Funktionen** geführt.

8) Da in einem Netzwerk alle internen Rufnummern eindeutig sein müssen, sind die Standard-Rufnummern zu löschen. Aktivieren Sie dazu das Optionsfeld **Alle Rufnummern löschen**.

9) Aktivieren Sie das Kontrollkästchen **Alle Rufnummern löschen** und klicken Sie auf **OK & Weiter**. Sie werden zum Fenster **Vorkonfigurierte Rufnummern ändern** geführt.

> ***INFO:*** Die Funktionskennzahlen müssen im Netzwerkverbund eindeutig sein. Doppelte Rufnummern sind nicht zulässig!

10) Passen Sie die vorkonfigurierten Rufnummern an die Rufnummern im Netzwerk an und klicken Sie auf **OK & Weiter**. Die Rufnummern können Sie entweder manuell über den Wizard anpassen oder Sie importieren eine CSV-Datei mit den entsprechend vorbereiteten Rufnummern.

11) Importieren Sie die IP-Clients.

12) Konfigurieren Sie jetzt die Internet-Telefonie.

13) Ändern Sie die Einstellungen für eine MeetMe-Konferenz. Sie müssen eine eindeutige Kennzahl im Netzwerkverbund eingeben.

14) Konfigurieren Sie jetzt den E-Mail-Versand.

15) Klicken Sie auf **OK & Weiter**.

16) Klicken Sie auf **Beenden**.

20.6.7.2 Wie Sie die Vernetzung für Knoten 1 (Master) konfigurieren

Im nächsten Schritt wird der Wizard für die Vernetzung von Knoten 1 (Master) konfiguriert.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Grundinstallation**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Vernetzung-Konfiguration** zu starten.

4) Wählen Sie die Einstellung **Netzwerk mit OSBiz X / OSBiz S**.

5) Definieren Sie den Knotentyp (**Master**).

6) Geben Sie unter **Node-ID** die entsprechenden Knotennummern der zugehörigen OpenScape Business Systeme ein (im Einrichtebeispiel die des Slaves mit der Node-ID 2).

7) Geben Sie unter **IP-Adresse** die IP-Adressen der zugehörigen OpenScape Business Systeme ein (im Einrichtebeispiel die der Slaves mit der Node-ID 2 und 3).

8) Aktivieren Sie das Kontrollkästchen **Gateway**.

9) Geben Sie unter **Name** die Art der Anlage ein.

10) Geben Sie unter **Typ** den Typ der Unteranlage ein.

11) Aktivieren Sie ggf. das Kontrollkästchen **Verschlüsselung**.

INFO: Die Verschlüsselung basiert auf SPE und gilt nicht für die Applikationen!

HINWEIS: Durch die Aktivierung des Kontrollkästchens ist noch keine Verschlüsselung konfiguriert. Siehe *Signaling and Payload Encryption SPE*.

---

12) Klicken Sie auf **Beenden**.

20.6.7.3 Wie Sie die Basisinstallation für Knoten 2 (Slave) konfigurieren

Für die Integration in einen Netzwerkverbund müssen die Ländervorwahl und eine Knoten-ID zugewiesen werden. Die internen Rufnummern müssen netzweit eindeutig konfiguriert werden. Die Eingabe der nationalen und lokalen Rufnummern ist wichtig, da diese Rufnummer in der Rtg1 ISDN Amt eingestellt wird und zur Normalisierung als Standortrufnummer verwendet wird.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Basisinstallation**.

3) Geben Sie im Feld **Ländervorwahl** die Ländervorwahl ein, z. B. 49 für Deutschland.

4) Tragen Sie die **Ortskennzahl** und **Anlagenrufnummer** ein.

5) Aktivieren Sie das Kontrollkästchen **Netzwerk-Integration**.

6) Vergeben Sie im Feld **Knoten-ID** für eine OpenScape Business eine im Netzverbund eindeutige Knoten-ID (eine "**2**" und eine "**3**" für das Einrichtebeispiel).

7) Klicken Sie auf **Funktion ausführen**. Sie werden zum Fenster **Zentrale Teilnehmer-Funktionen** geführt.

8) Da in einem Netzwerk alle internen Rufnummern eindeutig sein müssen, sind die Standard-Rufnummern zu löschen. Aktivieren Sie dazu das Optionsfeld **Alle Rufnummern löschen**.

9) Aktivieren Sie das Kontrollkästchen **Alle Rufnummern löschen** und klicken Sie auf **OK & Weiter**. Sie werden zum Fenster **Vorkonfigurierte Rufnummern ändern** geführt.

> ***INFO:*** Die Funktionskennzahlen müssen im Netzwerkverbund eindeutig sein. Doppelte Rufnummern sind nicht zulässig!

10) Passen Sie die vorkonfigurierten Rufnummern an die Rufnummern im Netzwerk an und klicken Sie auf **OK & Weiter**. Die Rufnummern können Sie entweder manuell über den Wizard anpassen oder Sie importieren eine CSV-Datei mit den entsprechend vorbereiteten Rufnummern.

11) Konfigurieren Sie jetzt die ISDN- und analogen Teilnehmer.

12) Ändern Sie die Einstellungen für eine MeetMe-Konferenz. Sie müssen eine eindeutige Kennzahl im Netzwerkverbund eingeben.

13) Konfigurieren Sie jetzt den E-Mail-Versand.

14) Klicken Sie auf **OK & Weiter**.

15) Klicken Sie auf **Beenden**.

20.6.7.4 Wie Sie die Vernetzung für Knoten 2 (Slave) konfigurieren

Im nächsten Schritt wird über den Wizard die Vernetzung von Knoten 2 konfiguriert.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards > Grundinstallation**.
3) Klicken Sie auf **Bearbeiten**, um den Wizard **Vernetzung-Konfiguration** zu starten.
4) Wählen Sie die Einstellung **Netzwerk mit OSBiz X / OSBiz S**.
5) Aktivieren Sie unter **Knotentyp** das Kästchen **Dieses System ist ein SLAVE-Knoten**.
6) **Geben Sie die IP-Adresse des MASTER-Knotens ein** (im Einrichtebeispiel die IP-Adresse von Knoten 1).

   INFO: Nach dem Klicken von **OK & Weiter** kann diese Aktion nicht mehr rückgängiggemacht werden!

7) Der **Registrierungsstatus** wird mit **Status erfolgreich** angezeigt (oder mit entsprechender Fehlermeldung). Damit ist der Wizard abgeschlossen.
8) Klicken Sie auf **Beenden**.

20.6.7.5 Wie Sie die Basisinstallation für Knoten 3 (Slave) konfigurieren

Für die Integration in einen Netzwerkverbund müssen die Ländervorwahl und eine Knoten-ID zugewiesen werden. Die internen Rufnummern müssen netzweit eindeutig konfiguriert werden. Die Eingabe der nationalen und lokalen Rufnummern ist wichtig, da diese Rufnummer in der Rtg1 ISDN Amt eingestellt wird und zur Normalisierung als Standortrufnummer verwendet wird.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
2) Klicken Sie im Navigationsbaum auf **Wizards > Basisinstallation**.
3) Geben Sie im Feld **Ländervorwahl** die Ländervorwahl ein, z. B. 49 für Deutschland.
4) Tragen Sie die **Ortskennzahl** und **Anlagenrufnummer** ein (identisch mit dem zugeordneten Gateway-System).
5) Aktivieren Sie das Kontrollkästchen **Netzwerk-Integration**.
6) Vergeben Sie im Feld **Knoten-ID** für eine OpenScape Business eine im Netzverbund eindeutige Knoten-ID (eine "**3**" für das Einrichtebeispiel).
7) Klicken Sie auf **Funktion ausführen**. Sie werden zum Fenster **Zentrale Teilnehmer-Funktionen** geführt.

8) Da in einem Netzwerk alle internen Rufnummern eindeutig sein müssen, sind die Standard-Rufnummern zu löschen. Aktivieren Sie dazu das Optionsfeld **Alle Rufnummern löschen**.

9) Aktivieren Sie das Kontrollkästchen **Alle Rufnummern löschen** und klicken Sie auf **OK & Weiter**. Sie werden zum Fenster **Vorkonfigurierte Rufnummern ändern** geführt.

> ***INFO:*** Die Funktionskennzahlen müssen im Netzwerkverbund eindeutig sein. Doppelte Rufnummern sind nicht zulässig!

10) Passen Sie die vorkonfigurierten Rufnummern an die Rufnummern im Netzwerk an und klicken Sie auf **OK & Weiter**. Die Rufnummern können Sie entweder manuell über den Wizard anpassen oder Sie importieren eine CSV-Datei mit den entsprechend vorbereiteten Rufnummern.

11) Konfigurieren Sie jetzt die ISDN- und analogen Teilnehmer.

12) Ändern Sie die Einstellungen für eine MeetMe-Konferenz. Sie müssen eine eindeutige Kennzahl im Netzwerkverbund eingeben.

13) Konfigurieren Sie jetzt den E-Mail-Versand.

14) Klicken Sie auf **OK & Weiter**.

15) Klicken Sie auf **Beenden**.

20.6.7.6 Vernetzung konfigurieren für Knoten 3 (Slave)

Im nächsten Schritt wird über den Wizard für die Vernetzung von Knoten 3 konfiguriert.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Grundinstallation**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Vernetzung-Konfiguration** zu starten.

4) Wählen Sie die Einstellung **Netzwerk mit OSBiz X / OSBiz S**.

5) Aktivieren Sie unter **Knotentyp** das Kästchen **Dieses System ist ein SLAVE-Knoten**.

6) **Geben Sie die IP-Adresse des MASTER-Knotens ein** (im Einrichtebeispiel die IP-Adresse von Knoten 1).

INFO: Nach dem Klicken von **OK & Weiter** kann diese Aktion nicht mehr rückgängiggemacht werden!

7) Der **Registrierungsstatus** wird mit **Status erfolgreich** angezeigt (oder mit entsprechender Fehlermeldung). Damit ist der Wizard abgeschlossen.

8) Klicken Sie auf **Beenden**.

20.6.7.7 Wie Sie die Vernetzungsfunktion für den Master kontrollieren

Sie können den Status der Vernetzung generell und die einzelnen Rufnummern kontrollieren.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Netzwerk**.

2) In der Statuszeile sehen Sie den **Synchronisationsstatus** für das Netzwerk. Grün bedeutet, dass die Vernetzung keine Probleme hat, Rot bedeutet Probleme im Netzwerk.

3) Markieren Sie im Fenster **Netzwerk** die Registerkarte **Knoten-Sicht** und es werden alle verfügbaren Knoten mit **Knoten ID**, **Name**, **System Typ**, **Server Adresse**, **Registrierungsstatus** und **Verfügbarkeitsstatus** angezeigt.

4) Markieren sie im Fenster **Netzwerk** die Registerkarte **Rufnummern** und es öffnet sich ein Fenster mit allen Angaben zu:

Rufnummer
DuWa
Name
Port Typ
Knoten

20.6.7.8 Wie Sie LCR für die Vernetzung konfigurieren (Knoten 3, Slave)

Im LCR Wahlplan sind die Default-Einträge im Index 32, 33, 34 und 35 um weitere Einträge für die Wahl von Rufnummern im Format "International, National und Teilnehmer" zu den Knoten 1 und 2 zu ergänzen. "International" und "National" werden immer benötigt, "Teilnehmer" nur für Partnerknoten, die sich im gleichen Ortsnetz befinden. Die Einträge 36, 37 und 39 für das Interworking mit Knoten 1 (Rufnummer 100 > 199) und die Einträge 39, 40 und 41 für das Interworking mit Knoten 2 (Rufnummer 200 > 299) sind zu ergänzen. Diese Angaben werden für die Wahl aus Applikationen (z. B. myPortal for Desktop) verwendet.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > LCR**.

3) Klicken Sie im Menübaum auf **Wahlplan**.

4) Geben Sie folgende Werte auf freien Plätzen (hier 35 bis 40) nach den Standardwerten ein:

Wahlplan	Name	Gewählte Ziffern	Wegetabelle
31	Appl-Suite	-371	12
32	Standard	88CZ	1
33	IP-Network	-Z	13
34	COInternat	0C0049-Z	14
36	Knoten 1 Inter	0C0049230266719-1Z	16
37	Knoten 1 Nat	0C0230266719-1Z	16
38	Knoten 1 Teiln.	0C66719-1Z	16
39	Knoten 2 Inter	0C0049230266719-2Z	17
40	Knoten 2 Nat	0C0230266719-2Z	17
41	Knoten 2 Teiln.	0C66719-2Z	17

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

6) Klicken Sie im Menübaum auf die zugehörige **Wahlregel** für Knoten 1 und 2.

a) Geben Sie unter **Regelname** den Eintrag **Knoten 1 + 2** ein.

b) Geben Sie unter **Wahlregelformat** den Eintrag **D49230266719E3A** ein.

c) Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus.

d) Wählen Sie unter **Type** den Eintrag **Ländervorwahl** aus.

e) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

7) Klicken Sie im Menübaum auf **Wegetabelle**, um die Wegetabelle 16 für das Networking zu konfigurieren und dem Knoten 1 direkt zuzuordnen.

8) Klicken Sie auf die Wegetabelle 16.

a) Wählen Sie unter **Richtung** den Eintrag **Networking** aus.

b) Wählen Sie unter **Wahlregel** den Eintrag **Knoten 1 + 2** aus.

c) Wählen Sie unter **Min. Ber.** den Eintrag **15** aus.

d) Wählen Sie unter **Warnung** den Eintrag **Keine** aus.

e) Wählen Sie unter **Dediziertes Gateway** den Eintrag **Erzwungen** aus.

f) Wählen Sie unter **GW Knoten-ID** den Eintrag **1** aus.

g) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9) Klicken Sie im Menübaum auf **Wegetabelle**, um eine Wegetabelle 17 für das Networking zu konfigurieren und dem Knoten 2 direkt zuzuordnen.

10) Klicken Sie auf die Wegetabelle 17.

a) Wählen Sie unter **Richtung** den Eintrag **Networking** aus.

b) Wählen Sie unter **Wahlregel** den Eintrag **Knoten 1 + 2** aus.

c) Wählen Sie unter **Min. Ber.** den Eintrag **15** aus.

d) Wählen Sie unter **Warnung** den Eintrag **Keine** aus.

e) Wählen Sie unter **Dediziertes Gateway** den Eintrag **Erzwungen** aus.

f) Wählen Sie unter **GW Knoten-ID** den Eintrag **2** aus.

g) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

20.6.7.9 Wie Sie LCR für die Vernetzung konfigurieren (Knoten 2)

Im LCR Wahlplan sind die Default-Einträge im Index 32, 33, 34 und 35 um weitere Einträge für die Wahl von Rufnummern im Format "International, National und Teilnehmer" zu den Knoten 1 und 3 zu ergänzen. "International" und "National" werden immer benötigt, "Teilnehmer" nur für Partnerknoten, die sich im gleichen Ortsnetz befinden. Die Einträge 36, 37 und 38 für das Interworking mit Knoten 1 (Rufnummer 100 > 199) und die Einträge 39, 40 und 41 für das Interworking mit Knoten 3 (Rufnummer 300 > 399) sind zu ergänzen. Diese Angaben werden für die Wahl aus Applikationen (z. B. myPortal for Desktop) verwendet.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > LCR**.

3) Klicken Sie im Menübaum auf **Wahlplan**.

4) Geben Sie folgende Werte auf freien Plätzen (hier 35 bis 40) nach den Standardwerten ein:

Wahlplan	Name	Gewählte Ziffern	Wegetabelle
31	Appl-Suite	-271	12
32	Standard	88CZ	1
33	IP-Network	-Z	13
34	COInternat	0C0049-Z	14
36	Knoten 1 Inter	0C0049230266719-1Z	16

Wahlplan	Name	Gewählte Ziffern	Wegetabelle
37	Knoten 1 Nat	0C0230266719-1Z	16
38	Knoten 1 Teiln.	0C66719-1Z	16
39	Knoten 3 Inter	0C0049230266758-3Z	17
40	Knoten 3 Nat	0C0230266758-3Z	17
41	Knoten 3 Teiln.	0C66758-3Z	17

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

6) Klicken Sie im Menübaum auf **Wegetabelle**.

7) Klicken Sie im Menübaum auf die zugehörige **Wahlregel** für Knoten 1.

- ***a)*** Geben Sie unter **Regelname** den Eintrag **Knoten 1** ein.
- ***b)*** Geben Sie unter **Wahlregelformat** den Eintrag **D49230266719E3A** ein.
- ***c)*** Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus.
- ***d)*** Wählen Sie unter **Type** den Eintrag **Ländervorwahl** aus.
- ***e)*** Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

8) Klicken Sie auf die Wegetabelle 16, um diese für das Networking zum Knoten 1 zu konfigurieren.

- ***a)*** Wählen Sie unter **Richtung** den Eintrag **Networking** aus.
- ***b)*** Wählen Sie unter **Wahlregel** den Eintrag **Knoten 1** aus.
- ***c)*** Wählen Sie unter **Min. Ber.** den Eintrag **1** aus.
- ***d)*** Wählen Sie unter **Warnung** den Eintrag **Keine** aus.
- ***e)*** Wählen Sie unter **Dediziertes Gateway** den Eintrag **Erzwungen** aus.
- ***f)*** Wählen Sie unter **GW Knoten-ID** den Eintrag **1** aus.
- ***g)*** Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9) Klicken Sie im Menübaum auf die zugehörige **Wahlregel** für Knoten 3.

- ***a)*** Geben Sie unter **Regelname** den Eintrag **Knoten 3** ein.
- ***b)*** Geben Sie unter **Wahlregelformat** den Eintrag **D49230266758E3A** ein.
- ***c)*** Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus.
- ***d)*** Wählen Sie unter **Type** den Eintrag **Ländervorwahl** aus.
- ***e)*** Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10) Klicken Sie im Menübaum auf **Wegetabelle**.

11) Klicken Sie auf die Wegetabelle 17, um diese für das Networking zum Knoten 3 zu konfigurieren.

- ***a)*** Wählen Sie unter **Richtung** den Eintrag **Networking** aus.
- ***b)*** Wählen Sie unter **Wahlregel** den Eintrag **Knoten 3** aus.

c) Wählen Sie unter **Min. Ber.** den Eintrag **1** aus.

d) Wählen Sie unter **Warnung** den Eintrag **Keine** aus.

e) Wählen Sie unter **Dediziertes Gateway** den Eintrag **Erzwungen** aus.

f) Wählen Sie unter **GW Knoten-ID** den Eintrag **3** aus.

g) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

20.6.7.10 Wie Sie Richtungen und Richtungsparameter konfigurieren (Knoten 1, Master)

Im Knoten 1 sind die Einstellungen für die Amtsrichtung bzgl. Standort-Nummer, Richtungskennzahl und Richtungsparameter zu konfigurieren. Hier muss die Anlagenrufnummer zur Definition des Gateway-Standortes eingetragen sein. Diese Angaben werden für die Wahl aus Applikationen wie z. B. MyPortal verwendet.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Leitungen/Vernetzung**.

3) Klicken Sie im Menübaum auf **Richtung**.

4) Geben Sie im Fenster **Richtung ändern** im Feld **Richtungsname** einen Namen `Rtg. 1` für die Amtsrichtung ein.

5) Geben Sie unter **Richtungskennzahl** die `0` ein.

6) Geben Sie unter **Anlagenrufnummer-kommend** im Feld **Ländervorwahl** die `49` ein.

7) Geben Sie unter **Anlagenrufnummer-kommend** im Feld **Ortsnetzkennzahl** die `2302` ein.

8) Geben Sie unter **Anlagenrufnummer-kommend** im Feld **Anlagenrufnummer** die `66719` ein.

9) Markieren Sie das Kontrollkästchen unter **Anlagenrufnummer-kommend** im Feld **Standort-Nummer**.

10) Die Default-Einstellungen für die Richtungsparameter (Nr.-Typ, gehen, Rufnummer Typ) können übernommen werden.

11) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

20.6.7.11 Wie Sie Richtungen und Richtungsparameter (Rtg. 16) konfigurieren (Knoten 1)

Für die Richtung 16 (Networking) ist es für Master und Slave zwingend erforderlich, den Eintrag für das 2. AKZ auszufüllen.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Leitungen/Vernetzung**.

3) Klicken Sie im Menübaum auf die letzte **Richtung** (**Rtg. 16**).

4) Geben Sie im Fenster **Richtung ändern** im Feld **Richtungsname** einen Namen `Networking` für die Vernetzungsrichtung ein.

5) Geben Sie unter **Richtungskennzahl** nichts ein.

6) Geben Sie unter **Amtskennziffer (2. AKZ)** die 0 ein.

7) Die Default-Einstellungen für die Richtungsparameter (Nr.-Typ, gehen, Rufnummer Typ) können übernommen werden.

8) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

20.6.7.12 Wie Sie LCR für die Vernetzung konfigurieren (Knoten 1)

Im LCR Wahlplan sind die Default-Einträge im Index 32, 33, 34 und 35 um weitere Einträge für die Wahl von Rufnummern im Format "International, National und Teilnehmer" zu den Knoten 2 und 3 zu ergänzen. "International" und "National" werden immer benötigt, "Teilnehmer" nur für Partnerknoten, die sich im gleichen Ortsnetz befinden. Diese Angaben werden für die Wahl aus Applikationen (z. B. myPortal for Desktop) verwendet.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > LCR**.

3) Klicken Sie im Menübaum auf **Wahlplan**.

4) Geben Sie folgende Werte auf freien Plätzen (hier 35 bis 40) nach den Standardwerten ein:

Wahlplan	Name	Gewählte Ziffern	Wegetabelle
16	Standard	0CZ	1
17	Standard	0C1Z	1
18	Standard	0CNZ	1
32	Standard	88CZ	1
33	IP-Network	-Z	13
34	COInternat	0C0049-Z	14
36	Knoten 2 Inter	0C0049230266719-2Z	16
37	Knoten 2 Nat	0C0230266719-2Z	16
38	Knoten 2 Teiln.	0C66719-2Z	16
39	Knoten 3 Inter	0C0049230266758-3Z	17
40	Knoten 3 Nat	0C0230266758-3Z	17
41	Knoten 3 Teiln.	0C66758-3Z	17

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

6) Klicken Sie im Menübaum auf die zugehörige **Wahlregel** für Knoten 2.

- ***a)*** Geben Sie unter **Regelname** den Eintrag **Knoten 2** ein.
- ***b)*** Geben Sie unter **Wahlregelformat** den Eintrag **D49230266719E3A** ein.
- ***c)*** Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus.
- ***d)*** Wählen Sie unter **Type** den Eintrag **Ländervorwahl** aus.
- ***e)*** Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

7) Klicken Sie im Menübaum auf **Wegetabelle**.

8) Klicken Sie auf die Wegetabelle 16, um diese für das Networking zum Knoten 2 zu konfigurieren.

- ***a)*** Wählen Sie unter **Richtung** den Eintrag **Networking** aus.
- ***b)*** Wählen Sie unter **Wahlregel** den Eintrag **Knoten 2** aus.
- ***c)*** Wählen Sie unter **Min. Ber.** den Eintrag **1** aus.
- ***d)*** Wählen Sie unter **Warnung** den Eintrag **Keine** aus.
- ***e)*** Wählen Sie unter **Dediziertes Gateway** den Eintrag **Erzwungen** aus.
- ***f)*** Wählen Sie unter **GW Knoten-ID** den Eintrag **2** aus.
- ***g)*** Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9) Klicken Sie im Menübaum auf die zugehörige **Wahlregel** für Knoten 3.

- ***a)*** Geben Sie unter **Regelname** den Eintrag **Knoten 3** ein.
- ***b)*** Geben Sie unter **Wahlregelformat** den Eintrag **D49230266719E1A** ein.

c) Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus.

d) Wählen Sie unter **Type** den Eintrag **Ländervorwahl** aus.

e) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10) Klicken Sie im Menübaum auf **Wegetabelle**.

11) Klicken Sie auf die Wegetabelle 17, um diese für das Networking zum Knoten 3 zu konfigurieren.

a) Wählen Sie unter **Richtung** den Eintrag **Networking** aus.

b) Wählen Sie unter **Wahlregel** den Eintrag **Knoten 3** aus.

c) Wählen Sie unter **Min. Ber.** den Eintrag **1** aus.

d) Wählen Sie unter **Warnung** den Eintrag **Keine** aus.

e) Wählen Sie unter **Dediziertes Gateway** den Eintrag **Erzwungen** aus.

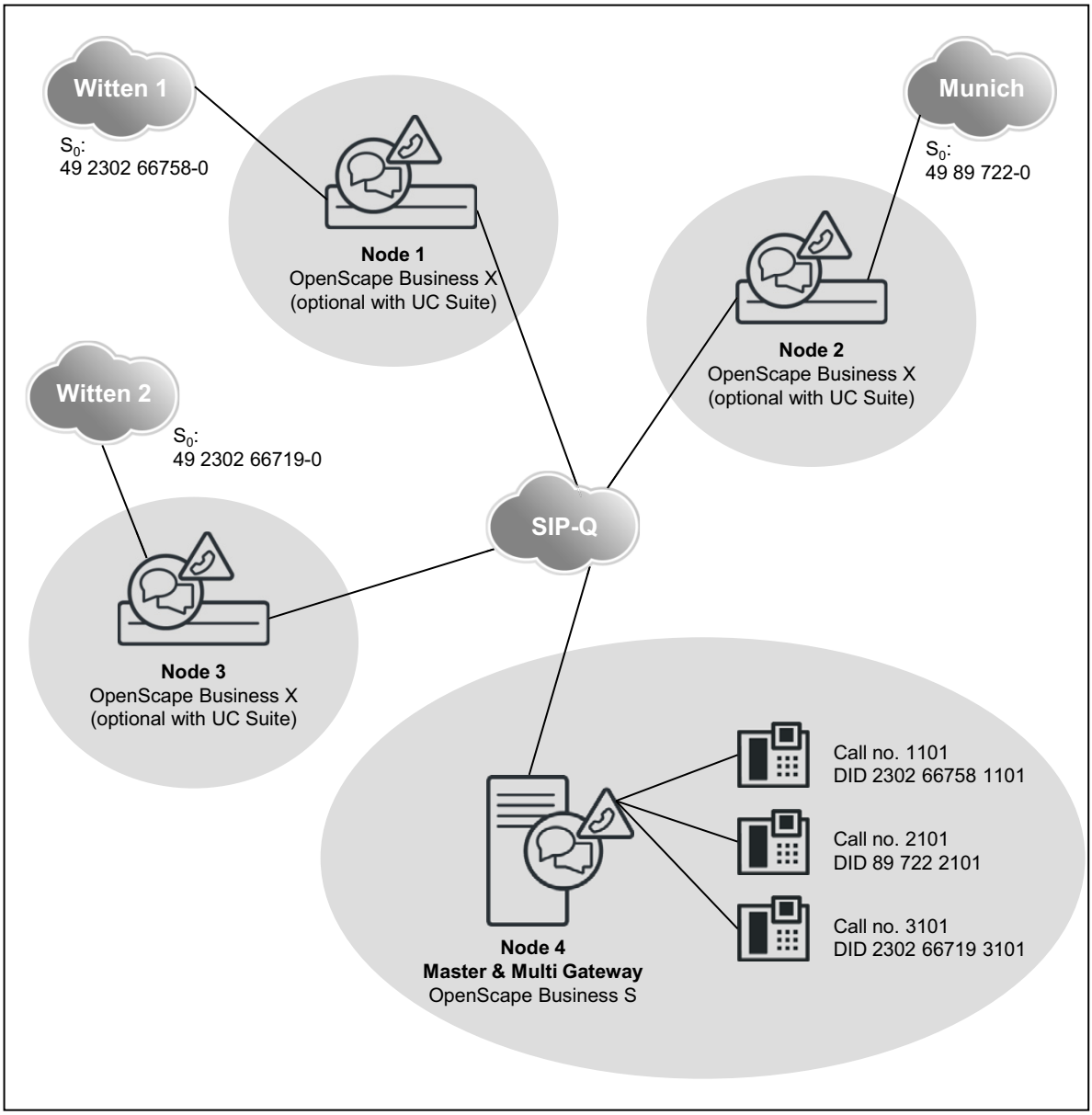
f) Wählen Sie unter **GW Knoten-ID** den Eintrag **3** aus.

g) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

12) Klicken Sie im Menübaum auf **Wegetabelle**.

20.6.8 Szenario 3: Vernetzung von Open Scape Business X und OpenScape Business S (Multi Gateway)

Bis zu 32 Kommunikationssysteme OpenScape Business X/S können miteinander vernetzt werden. Multi Gateway bedeutet, dass jeder an OpenScape Business S registrierte IP-Teilnehmer genau einem bestimmten Gateway zugeordnet sind.



Netzwerkdaten

- Geschlossene Nummerierung
- Netzweite Sprach- und UC-Funktionalität mit UC Suite Konfiguration über WBM (Wizards)
- Die UC-Funktionalität ist entweder über UC Booster Server oder über UC Booster Card realisiert
- Die UC-Funktionalität der OpenScape Business S ist integriert
- Es ist nur eine einzige OpenScape Business S im Netzverbund erlaubt.
- Alle Systeme müssen den gleichen Länder-Code benutzen
- Alle Systeme müssen sich in der gleichen Zeitzone befinden
- Es darf nur einen einzigen Amtszugangs-Code (z. B. 0) im Netz geben.

- Bis zu 32 vernetzte Systeme, 1000 User mit UC Smart (UC Smart Funktionen stehen knotenweit zur Verfügung)
- Bis zu 8 vernetzte Systeme, 1000 User mit UC Suite

20.6.9 Szenario 3: Netzweite Leistungsmerkmale

UC Vernetzung	Geschlossene Nummerierung	Offene Nummerierung
Maximale Anzahl Knoten	8 (mit UC Suite) und 32 (ohne UC Suite)	
Maximale Anzahl von Teilnehmern in einem einzelnen Kommunikationssystem	abhängig von OpenScape Business X	
Maximale Anzahl von Teilnehmern im Netz	1000	

UC Vernetzung	Geschlossene Nummerierung	Offene Nummerierung
UC Booster Server	ab 150 Teilnehmer	Wird nicht unterstützt
UC Booster Card	bis 150 Teilnehmer	Wird nicht unterstützt

Administration	Geschlossene Nummerierung	Offene Nummerierung
WBM	Netzweite Administration über Wizards	Wird nicht unterstützt
Manager E	Netzweite Administration für spezielle Aufgaben	Wird nicht unterstützt
UC-Suite-Administration (für UC Booster Server und UC Booster Card	Netzweite Administration über Wizards	Wird nicht unterstützt
Massendatenimport über csv-Dateien (Rufnummern, Durchwahlnummern, Namen)	Separat für jeden Knoten im Netzverbund	Wird nicht unterstützt

Lizenzierung	Geschlossene Nummerierung	Offene Nummerierung
Neue Lizenzierungsstruktur	Eine Vernetzungs-Lizenz für jeden Knoten erforderlich	Wird nicht unterstützt

myPortal for Desktop / myPortal for Outlook (UC Suite)	Geschlossene Nummerierung	Offene Nummerierung
	Netzweit mit UC-Funktionalität über UC Booster Server, UC Booster Card oder OpenScape Business S	Wird nicht unterstützt
Instant Messaging	Netzweit	Wird nicht unterstützt
VoiceMail	Die Teilnehmer nutzen ihr lokales VoiceMail-System; es gibt keine zentrale VoiceMail für den gesamten Netzverbund.	Wird nicht unterstützt
Anwesenheitsstatus	Netzweit	Wird nicht unterstützt

myPortal for Desktop / myPortal for Outlook (UC Suite)	Geschlossene Nummerierung	Offene Nummerierung
Besetztanzeige	Netzweit	Wird nicht unterstützt
Internes Verzeichnis / Favoriten	Netzweit	Wird nicht unterstützt
Externes Verzeichnis	Lokal über den Import von csv-Dateien	Wird nicht unterstützt
Suche in externen Verzeichnissen anderer Knoten	Nicht möglich	Wird nicht unterstützt
Externes Offline-Verzeichnis (LDAP)	über LDAP	Wird nicht unterstützt

myPortal Smart (UC Smart)	Geschlossene Nummerierung	Offene Nummerierung
	Netzweit	Wird nicht unterstützt
VoiceMail	Die Teilnehmer nutzen ihr lokales VoiceMail-System; es gibt keine zentrale VoiceMail für den gesamten Netzverbund.	Wird nicht unterstützt
Anwesenheitsstatus	Lokal	Wird nicht unterstützt
Besetztanzeige	Lokal	Wird nicht unterstützt
Internes Verzeichnis / Favoriten	Lokal	Wird nicht unterstützt

myAttendant	Geschlossene Nummerierung	Offene Nummerierung
	Mit UC-Funktionalität über UC Booster Server, UC Booster Card oder OpenScape Business S	Wird nicht unterstützt
Instant Messaging	Netzweit	Wird nicht unterstützt
VoiceMail	Die Teilnehmer nutzer ihr lokales VoiceMail-System; es gibt keine zentrale VoiceMail für den gesamten Netzverbund.	Wird nicht unterstützt
Anwesenheitsstatus	Netzweit	Wird nicht unterstützt
Besetztanzeige	Netzweit	Wird nicht unterstützt
Internes Verzeichnis / Favoriten	Netzweit	Wird nicht unterstützt
Externes Verzeichnis	Lokal über den Import von csv-Dateien	Wird nicht unterstützt
Suche in externen Verzeichnissen anderer Knoten	Nicht möglich	Wird nicht unterstützt
Externes Offline-Verzeichnis (LDAP)	über LDAP	Wird nicht unterstützt

myAttendant	Geschlossene Nummerierung	Offene Nummerierung
VoiceMail	Die Teilnehmer nutzer ihr lokales VoiceMail-System; es gibt keine zentrale VoiceMail für den gesamten Netzverbund.	Wird nicht unterstützt
VoiceMail-Abfrage für andere Teilnehmer	Lokal, nicht für Teilnehmer in anderen Knoten	Wird nicht unterstützt
Zentraler Vermittlungsplatz	Netzweit	Wird nicht unterstützt

OpenScape Business Attendant	Geschlossene Nummerierung	Offene Nummerierung
	Schnittstelle beschränkt auf 8-stellige Rufnummern	Wird nicht unterstützt
Anwesenheitsstatus	Netzweit über den BLF-Server	Wird nicht unterstützt
Besetztanzeige	Netzweit über den BLF-Server	Wird nicht unterstützt
Externes Verzeichnis	über LDAP	Wird nicht unterstützt
Zentraler Vermittlungsplatz	Netzweit	Wird nicht unterstützt

Company AutoAttendant (UC Suite)	Geschlossene Nummerierung	Offene Nummerierung
Company AutoAttendant: Nachdem der Auto-Attendant einen Anruf beantwortet hat, muss der Anrufer die Rufnummer wählen mit der er verbunden werden möchte.	ccv-Scripts erlauben es Rufnummern aus dem internen Verzeichnis innerhalb des Netzverbunds zu wählen.	Wird nicht unterstützt
Persönlicher AutoAttendant: Nachdem der AutoAttendant einen Anruf beantwortet hat, muss der Anrufer eine einstellige Ziffer wählen um mit seinem Anrufziel verbunden zu werden.	Jede von einem UC Teilnehmer vorkonfigurierte Rufnummer möglich	Wird nicht unterstützt

Company AutoAttendant (UC Smart)	Geschlossene Nummerierung	Offene Nummerierung
Company AutoAttendant	Lokal	Lokal

myAgent	Geschlossene Nummerierung	Offene Nummerierung
	Mit UC-Funktionalität über UC Booster Server, UC Booster Card oder OpenScape Business S. Alle Agenten sind an EINEM Knoten registriert. Eingehend CC-Anrufe über das lokale PSTN, ITSP und SIP-Q-Amtssätze.	Wird nicht unterstützt
VoiceMail (Aufnahme, Message Waiting Indication, Abfrage)	Die Teilnehmer nutzer ihr lokales VoiceMail-System; es gibt keine zentrale VoiceMail für den gesamten Netzverbund	Wird nicht unterstützt
Anwesenheitsstatus	Netzweit	Wird nicht unterstützt
Besetztanzeige	Netzweit	Wird nicht unterstützt

myAgent	Geschlossene Nummerierung	Offene Nummerierung
Agentenstatus	Lokal	Wird nicht unterstützt
Internes Verzeichnis / Favoriten	Netzweit	Wird nicht unterstützt
Externes Verzeichnis	Lokal über Import von csv-Dateien	Wird nicht unterstützt
Suche in externen Verzeichnissen anderer Knoten	Nicht möglich	Wird nicht unterstützt
Externes Offline-Verzeichnis (LDAP)	Lokal	Wird nicht unterstützt
Übergabe eines Anrufs	Lokal	Wird nicht unterstützt
Kundeninformation	Lokal	Wird nicht unterstützt
Reporting	Lokal	Wird nicht unterstützt

Externe Applikationen	Geschlossene Nummerierung	Offene Nummerierung
OpenScape Business TAPI-Applikationen	Siehe *Application Connectivity*	
Externe CSTA-Applikationen		
Application Launcher		
OpenScape Contact Center	Siehe *Multimedia Contact Center*.	

Telefonie	Geschlossene Nummerierung	Offene Nummerierung
SIP-Provider (ITSP)	Lokal	Lokal
PSTN-Provider	Lokal; Netzknoten ohne eigenen PSTN-Provider werden über SIP-Q bzw. das zugehörige Gateway erreicht.	Lokal
Survivability (Ausfallsicherheit im Falle eines Zusammenbruchs des Netzverbundes bzw. der OpenScape Business S)	Lokal	Lokal

Mobility	Geschlossene Nummerierung	Offene Nummerierung
Desksharing	Innerhalb eines Knotens; Netzweit mit DLS	Wird nicht unterstützt
Mobility mit DTMF-Steuerung des Systems	Lokal (wird bei OpenScape Business S nicht unterstützt)	
myPortal for Mobile (UC Suite)	Netzweiter Anwesenheitsstatus und Verzeichnisse (jeder Knoten benötigt dafür entweder UC Booster Server, UC Booster Card oder OpenScape Business S)	Wird nicht unterstützt
myPortal for Mobile (UC Smart)	Lokal, nicht für UC Booster Server, UC Booster Card und OpenScape Business S	Wird nicht unterstützt

Sonstige Funktionalitäten	Geschlossene Nummerierung	Offene Nummerierung
Signalling and Payload Encryption SPE	Wird nicht unterstützt bei UC-Verbindungen und Konferenzen	Wird nicht unterstützt bei Konferenzen
DSS-Server	Netzweit	Wird nicht unterstützt

20.6.10 Szenario 3: Konfiguration

Die Konfiguration von Szenario 3 (mit geschlossener Nummerierung und UC Suite) zeigt an einem Beispiel, welche Schritte für die Einrichtung einer Multi-Gateway Vernetzung durchzuführen sind.

Voraussetzungen:

- Es liegt ein Vernetzungsplan vor. Über den Vernetzungsplan ist sichergestellt, dass jede interne Rufnummer im Netzverbund bei verdeckter Nummerierung nur einmal vergeben ist. Unterschiedliche Rufnummernlängen sind zulässig. Nur Duwa-Rufnummern dürfen mehrfach vorkommen.
- Das IP-Netzwerk ist eingerichtet und alle Knoten können untereinander über Ping erreicht werden
- Alle Knoten sind auf die gleiche Softwareversion hochgerüstet

Knotenübergreifende Rufumleitungen: Bei kommenden Rufen über IP-Trunks, die bereits umgeleitet sind, werden weitere Umleitungen zur Sprachbox nicht ausgeführt. Hintergrund ist, dass ansonsten keine eindeutige Zuordnung zur Sprachbox erfolgen kann

Falls knotenübergreifende Stellvertreterregelungen gewünscht werden, sind diese über Profile der OpenScape Business Teilnehmer oder Rufzuschaltungen einzurichten. Entsprechende knotenübergreifende Anrufe werden in diesem Fall nicht als umgeleitet signalisiert, sondern als Direktruf. Daher werden Rufumleitungen des Stellvertreters zur Sprachbox umgeleitet

Einrichtung der Standortdaten für Knoten 1

Knoten 1		
G.-Standort Land		49
G.-Standort Ortsnetz		2302
G.-Standort Anlage		66758
Internationales Prefix		00
Nationales Prefix		0
Richtungen		
ISDN	AKZ	0
Networking	2. AKZ	0
Richtungsparameter		

Knoten 1		
Richtung	Nr-Typ gehend	RNR-Typ
Networking	Unbekannt	int/Duwa
ISDN	(Keine Änderung des Eintrags)	Duwa

In den Routingtabellen werden automatisch die Rufnummern aller Teilnehmer außerhalb von Knoten 1 eingetragen, und zwar die internen Rufnummern und die DID-Rufnummern, die sich von den jeweiligen internen Rufnummern unterscheiden.

Übersicht der Einträge im LCR für Knoten 1

Wahlplan		Wegetabelle			Wahlregel		
Name	**Gewählte Ziffern**	**Richtung**	**Dediziertes Gateway**	**Gateway ID**	**Wahlregel**	**Verfahren**	**Typ**
Knoten 2 Internat	0C004989722-Z	Networking	Erzwungen	2	D4989722E3A	Corp. Network	International
Knoten 2 NAT	0C089722-Z						
Knoten 2 Teiln.	0C722-Z						
Knoten 3 Internat	0C00492302667 19-Z	Networking	Erzwungen	3	D492302667 19E3A	Corp. Network	International
Knoten 3 NAT	0C0230266719-Z						
Knoten 3 Teiln.	0C66719-Z						
Knoten 4 Internat	0C00492302667 58-Z	Networking	NO		D230266758 E3A	Corp. Network	National
Knoten 4 NAT	0C0230266758-Z						
Knoten 4 Teiln.	0C66758-Z						
Diverse	-Z	Networking	No		BA	Corp. Network	Unknown
Amt International	0C0049-Z	ISDN	No		D0E3A	Hauptnetzanbieter	Unknown
Amt	0CZ	ISDN	No		A	Hauptnetzanbieter	Unknown

Einrichtung der Standortdaten für Knoten 2

Knoten 2	
G.-Standort Land	49
G.-Standort Ortsnetz	89
G.-Standort Anlage	722
Internationales Prefix	00
Nationales Prefix	0

Knoten 2		
Richtungen		
ISDN	AKZ	0
Networking	2. AKZ	0
Richtungsparameter		
Richtung	Nr-Typ gehend	RNR-Typ
Networking	Unbekannt	int/Duwa
ISDN	(Keine Änderung des Eintrags)	Duwa

In den Routingtabellen werden automatisch die Rufnummern aller Teilnehmer außerhalb von Knoten 2 eingetragen, und zwar die internen Rufnummern und die DID-Rufnummern, die sich von den jeweiligen internen Rufnummern unterscheiden.

Übersicht der Einträge im LCR für Knoten 2

Wahlplan		Wegetabelle			Wahlregel		
Name	**Gewählte Ziffern**	**Richtung**	**Dediziertes Gateway**	**Gateway ID**	**Wahlregel**	**Verfahren**	**Typ**
Knoten 1Internat	0C00492302667 58-Z	Networking	Erzwungen	1	D492302667 E3A	Corp. Network	International
Knoten 1NAT	0C0230266758-Z						
Knoten 1 Teiln.	0C66758-Z						
Knoten 3 Internat	0C00492302667 19-Z	Networking	Erzwungen	3	D492302667 19E3A	Corp. Network	International
Knoten 3 NAT	0C0230266719-Z						
Knoten 3 Teiln.	0C66719-Z						
Knoten 4 Internat	0C004989722-Z	Networking	NO		D89722E3A	Corp. Network	National
Knoten 4 NAT	0C089722-Z						
Knoten 4 Teiln.	0C722-Z						
Diverse	-Z	Networking	No		BA	Corp. Network	Unknown
Amt International	0C0049-Z	ISDN	No		D0E3A	Hauptnetzanbieter	Unknown
Amt	0CZ	ISDN	No		A	Hauptnetzanbieter	Unknown

Einrichtung der Standortdaten für Knoten 3

Knoten 3		
G.-Standort Land		49
G.-Standort Ortsnetz		2302
G.-Standort Anlage		66719
Internationales Prefix		00
Nationales Prefix		0
Richtungen		
ISDN	AKZ	0
Networking	2. AKZ	0
Richtungsparameter		
Richtung	Nr-Typ gehend	RNR-Typ
Networking	Unbekannt	int/Duwa
ISDN	(Keine Änderung des Eintrags)	Duwa

In den Routingtabellen werden automatisch die Rufnummern aller Teilnehmer außerhalb von Knoten 3 eingetragen, und zwar die internen Rufnummern und die DID-Rufnummern, die sich von den jeweiligen internen Rufnummern unterscheiden.

Übersicht der Einträge im LCR für Knoten 3

Wahlplan		Wegetabelle			Wahlregel		
Name	**Gewählte Ziffern**	**Richtung**	**Dediziertes Gateway**	**Gateway ID**	**Wahlregel**	**Verfahren**	**Typ**
Knoten 1Internat	0C00492302667 58-Z	Networking	Erzwungen	1	D492302667 58E3A	Corp. Network	International
Knoten 1 NAT	0C0230266758-Z						
Knoten 1 Teiln.	0C66758-Z						
Knoten 2 Internat	0C004989722-Z	Networking	Erzwungen	2	D4989722E3 A	Corp. Network	International
Knoten 2 NAT	0C089722-Z						
Knoten 2 Teiln.	0C722-Z						
Knoten 4 Internat	0C00498923026 6719-Z	Networking	No		D230266719 E3A	Corp. Network	National
Knoten 4 NAT	0C0230266719-Z						
Knoten 4 Teiln.	0C66719-Z						

Wahlplan		Wegetabelle			Wahlregel		
Name	**Gewählte Ziffern**	**Richtung**	**Dediziertes Gateway**	**Gateway ID**	**Wahlregel**	**Verfahren**	**Typ**
Diverse	-Z	Networking	No		BA	Corp. Network	Unknown
Amt International	0C0049-Z	ISDN	No		D0E3A	Hauptnetzanbieter	Unknown
Amt	0CZ	ISDN	No		A	Hauptnetzanbieter	Unknown

Einrichtung der Standortdaten für Knoten 4

Standortdaten an Pseudo-Amtsrichtung (Rtg. 1) inkl. Amtskennzahl = 0 und Typ = Amt binden, da der Knoten 4 keine direkte Anschaltung eines Amts hat.

Knoten 4, Pseudo-Amtsrichtung

Knoten 4		
G.-Standort Land		49
G.-Standort Ortsnetz		
G.-Standort Anlage		
Internationales Prefix		00
Nationales Prefix		0
Richtungen		
ISDN	AKZ	0
Networking	2. AKZ	0
Richtungsparameter		
Richtung	Nr-Typ gehend	RNR-Typ
Networking	Unbekannt	int/Duwa
ISDN	(Keine Änderung des Eintrags)	Duwa

In den Routingtabellen werden automatisch die Rufnummern aller Teilnehmer außerhalb von Knoten 1 eingetragen, und zwar die internen Rufnummern und die DID-Rufnummern, die sich von den jeweiligen internen Rufnummern unterscheiden.

Knoten 4, Richtung Networking

Knoten 4	
G.-Standort Land	
G.-Standort Ortsnetz	
G.-Standort Anlage	

Knoten 4		
Internationales Prefix		00
Nationales Prefix		0
Richtungen		
ISDN	AKZ	0
Networking	2. AKZ	0
Richtungsparameter		
Richtung	Nr-Typ gehend	RNR-Typ
Networking	National	int/Duwa
ISDN	(Keine Änderung des Eintrags)	Duwa

Übersicht der Einträge im LCR für Knoten 4

Wahlplan		Wegetabelle			Wahlregel		
Name	**Gewählte Ziffern**	**Richtung**	**Dediziertes Gateway**	**Gateway ID**	**Wahlregel**	**Verfahren**	**Typ**
Knoten 1Internat	0C0049230266758-Z	Networking	Erzwungen	1	D49230266758E3A	Corp. Network	International
Knoten 1 NAT	0C0230266758-Z						
Knoten 2 Internat	0C004989722-Z	Networking	Erzwungen	2	D4989722E3A	Corp. Network	International
Knoten 2 NAT	0C089722-Z						
Knoten 3 Internat	0C004989230266719-Z	Networking	Erzwungen	3	D49230266719E3A	Corp. Network	International
Knoten 3 NAT	0C0230266719-Z						
Diverse	-Z	Networking	NO		A	Corp. Network	Unknown
Amt	0CZ	Networking	MULTI-GATEWAY	1	E1A	Hauptnetzanbieter	Unknown

Vorgehensweise bei der Einrichtung der Vernetzung:

1. Basisinstallation für Knoten 4 (Master) konfigurieren
2. Vernetzung konfigurieren für Knoten 4 (Master)
3. Basisinstallation für Knoten 1 (Slave) konfigurieren
4. Vernetzung konfigurieren für Knoten 1 (Slave)
5. Basisinstallation für Knoten 2 (Slave) konfigurieren
6. Vernetzung konfigurieren für Knoten 2 (Slave)
7. Basisinstallation für Knoten 3 (Slave) konfigurieren
8. Vernetzung konfigurieren für Knoten 3 (Slave)
9. Vernetzungsfunktion kontrollieren für Master
10. Multi-Gateway konfigurieren für Knoten 4 (Master)

11. Richtungen und Richtungsparameter konfigurieren (Knoten 1, Slave)
12. LCR für die Vernetzung konfigurieren (Knoten 1, Slave)
13. Richtungen und Richtungsparameter konfigurieren (Knoten 2, Slave)
14. LCR für die Vernetzung konfigurieren (Knoten 2, Slave)
15. Richtungen und Richtungsparameter konfigurieren (Knoten 3, Slave)
16. LCR für die Vernetzung konfigurieren (Knoten 3, Slave)
17. Richtungen und Richtungsparameter konfigurieren (Knoten 4, Master)
18. LCR für die Vernetzung konfigurieren (Knoten 4, Master)

20.6.10.1 Wie Sie die Basisinstallation für Knoten 4 (OpenScape Business S, Master) konfigurieren

Für die Integration in einen Netzwerkverbund müssen die Ländervorwahl und eine Knoten-ID zugewiesen werden. Die internen Rufnummern müssen netzweit eindeutig konfiguriert werden. Die Eingabe der nationalen und lokalen Rufnummern ist wichtig, da diese Rufnummer in der Rtg1 ISDN Amt eingestellt wird und zur Normalisierung als Standortrufnummer verwendet wird.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Basisinstallation**.

3) Geben Sie im Feld **Ländervorwahl** die Ländervorwahl ein, z. B. 49 für Deutschland.

4) Machen Sie keine Eintragungen für die Felder **Ortskennzahl** und **Anlagen-rufnummer**!.

5) Aktivieren Sie das Kontrollkästchen **Netzwerk-Integration**.

6) Vergeben Sie im Feld **Knoten-ID** für OpenScape Business S eine im Netzverbund eindeutige Knoten-ID. Die Knoten-Id muss zwischen "**1**" und "**100**" sein (eine "**4**" wurde für das Einrichtebeispiel vergeben).

7) Klicken Sie auf **Funktion ausführen**. Sie werden zum Fenster **Zentrale Teilnehmer-Funktionen** geführt.

8) Da in einem Netzwerk alle internen Rufnummern eindeutig sein müssen, sind die Standard-Rufnummern zu löschen. Aktivieren Sie dazu das Optionsfeld **Alle Rufnummern löschen**.

9) Aktivieren Sie das Kontrollkästchen **Alle Rufnummern löschen** und klicken Sie auf **OK & Weiter**. Sie werden zum Fenster **Vorkonfigurierte Rufnummern ändern** geführt.

INFO: Die Funktionskennzahlen müssen im Netzwerkverbund eindeutig sein. Doppelte Rufnummern sind nicht zulässig!

10) Passen Sie die vorkonfigurierten Rufnummern an die Rufnummern im Netzwerk an und klicken Sie auf **OK & Weiter**. Die Rufnummern können Sie entweder manuell über den Wizard anpassen oder Sie importieren eine CSV-Datei mit den entsprechend vorbereiteten Rufnummern.

11) Importieren Sie jetzt die IP-Clients.

12) Konfigurieren Sie die IP-Clients.

13) Ändern Sie die Einstellungen für eine MeetMe-Konferenz. Sie müssen eine eindeutige Kennzahl im Netzwerkverbund eingeben.

14) Konfigurieren Sie jetzt den E-Mail-Versand.

15) Klicken Sie auf **Beenden**.

20.6.10.2 Wie Sie die Vernetzung für Knoten 4 (Master) konfigurieren

Im nächsten Schritt wird über den Wizard für die Vernetzung von Knoten 3 konfiguriert.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Grundinstallation**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Vernetzung-Konfiguration** zu starten.

4) Wählen Sie die Einstellung **Netzwerk mit OSBiz X / OSBiz S**.

5) Aktivieren Sie das Kontrollkästchen **Dieses System ist der Master-Knoten**.

6) Geben Sie unter **Node-ID** die entsprechenden Knotennummern der zugehörigen OpenScape Business Systeme ein (im Einrichtebeispiel die der Slaves mit der Node-ID 1, 2 und 3).

7) Geben Sie unter **IP-Adresse** die IP-Adressen der zugehörigen OpenScape Business Systeme ein (im Einrichtebeispiel die der Slaves mit der Node-ID 1, 2 und 3).

8) Aktivieren Sie das Kontrollkästchen **Gateway**.

9) Geben Sie unter **Name** die Art der Anlage (z. B. Slave 1) ein.

10) Geben Sie unter **Typ** den Typ der Unteranlage ein.

11) Aktivieren Sie ggf. das Kontrollkästchen **Verschlüsselung**.

INFO: Die Verschlüsselung basiert auf SPE und gilt nicht für die Applikationen!

HINWEIS: Durch die Aktivierung des Kontrollkästchens ist noch keine Verschlüsselung konfiguriert. Siehe *Signaling and Payload Encryption SPE*.

12) Klicken Sie auf **Beenden**.

20.6.10.3 Wie Sie die Basisinstallation für Knoten 1 (Slave) konfigurieren

Für die Integration in einen Netzwerkverbund müssen die Ländervorwahl und eine Knoten-ID zugewiesen werden. Die internen Rufnummern müssen netzweit eindeutig konfiguriert werden. Die Eingabe der nationalen und lokalen Rufnummern ist wichtig, da diese Rufnummer in der Rtg1 ISDN Amt eingestellt wird und zur Normalisierung als Standortrufnummer verwendet wird.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Basisinstallation**.

3) Geben Sie im Feld **Ländervorwahl** die Ländervorwahl ein, z. B. 49 für Deutschland.

4) Tragen Sie die **Ortskennzahl** und **Anlagenrufnummer** ein.

5) Aktivieren Sie das Kontrollkästchen **Netzwerk-Integration**.

6) Vergeben Sie im Feld **Knoten-ID** für OpenScape Business S eine im Netzverbund eindeutige Knoten-ID (eine "**1**" für das Einrichtebeispiel).

7) Klicken Sie auf **Funktion ausführen**. Sie werden zum Fenster **Zentrale Teilnehmer-Funktionen** geführt.

8) Da in einem Netzwerk alle Rufnummern eindeutig sein müssen, sind die Standard-Rufnummern zu löschen. Aktivieren Sie dazu das Optionsfeld **Alle Rufnummern löschen**.

9) Aktivieren Sie das Kontrollkästchen **Alle Rufnummern löschen** und klicken Sie auf **OK & Weiter**. Sie werden zum Fenster **Vorkonfigurierte Rufnummern ändern** geführt.

INFO: Die Funktionskennzahlen müssen im Netzwerkverbund eindeutig sein. Doppelte Rufnummern sind nicht zulässig!

10) Passen Sie die vorkonfigurierten Rufnummern an die Rufnummern im Netzwerk an und klicken Sie auf **OK & Weiter**. Die Rufnummern können Sie entweder manuell über den Wizard anpassen oder Sie importieren eine CSV-Datei mit den entsprechend vorbereiteten Rufnummern.

11) Konfigurieren Sie jetzt die ISDN- und analogen Teilnehmer.

12) Ändern Sie die Einstellungen für eine MeetMe-Konferenz. Sie müssen eine eindeutige Kennzahl im Netzwerkverbund eingeben.

13) Konfigurieren Sie jetzt den E-Mail-Versand.

14) Klicken Sie auf **Beenden**.

20.6.10.4 Wie Sie die Vernetzung für Knoten 1 (Slave) konfigurieren

Im nächsten Schritt wird der Wizard für die Vernetzung konfiguriert.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Grundinstallation**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Vernetzung-Konfiguration** zu starten.

4) Wählen Sie die Einstellung **Netzwerk mit OSBiz X / OSBiz S**.

5) **Geben Sie die IP-Adresse des MASTER-Knotens ein** (Eine OpenScape Business wird als Slave-Knoten eingerichtet und die entsprechende IP-Adresse des Master-Knotens, der OpenScape Business S, eingetragen. Master und Multi-Gateway werden immer dem gleichen System, im Einrichtebeispiel der OpenScape Business S zugeordnet).

> ***INFO:*** Nach dem Klicken von **OK & Weiter** kann diese Aktion nicht mehr rückgängiggemacht werden!

6) Der **Registrierungsstatus** wird mit **Status erfolgreich** angezeigt (oder mit entsprechender Fehlermeldung). Damit ist der Wizard abgeschlossen.

7) Klicken Sie auf **Beenden**.

20.6.10.5 Wie Sie die Basisinstallation für Knoten 2 (Slave) konfigurieren

Für die Integration in einen Netzwerkverbund müssen die Ländervorwahl und eine Knoten-ID zugewiesen werden. Die internen Rufnummern müssen netzweit eindeutig konfiguriert werden. Die Eingabe der nationalen und lokalen

Rufnummern ist wichtig, da diese Rufnummer in der Rtg1 ISDN Amt eingestellt wird und zur Normalisierung als Standortrufnummer verwendet wird.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Basisinstallation**.

3) Geben Sie im Feld **Ländervorwahl** die Ländervorwahl ein, z. B. 49 für Deutschland.

4) Tragen Sie die **Ortskennzahl** und **Anlagenrufnummer** ein.

5) Aktivieren Sie das Kontrollkästchen **Netzwerk-Integration**.

6) Vergeben Sie im Feld **Knoten-ID** für OpenScape Business S eine im Netzverbund eindeutige Knoten-ID (eine "**2**" für das Einrichtebeispiel).

7) Klicken Sie auf **Funktion ausführen**. Sie werden zum Fenster **Zentrale Teilnehmer-Funktionen** geführt.

8) Da in einem Netzwerk alle internen Rufnummern eindeutig sein müssen, sind die Standard-Rufnummern zu löschen. Aktivieren Sie dazu das Optionsfeld **Alle Rufnummern löschen**.

9) Aktivieren Sie das Kontrollkästchen **Alle Rufnummern löschen** und klicken Sie auf **OK & Weiter**. Sie werden zum Fenster **Vorkonfigurierte Rufnummern ändern** geführt.

> ***INFO:*** Die Funktionskennzahlen müssen im Netzwerkverbund eindeutig sein. Doppelte Rufnummern sind nicht zulässig!

10) Passen Sie die vorkonfigurierten Rufnummern an die Rufnummern im Netzwerk an und klicken Sie auf **OK & Weiter**. Die Rufnummern können Sie entweder manuell über den Wizard anpassen oder Sie importieren eine CSV-Datei mit den entsprechend vorbereiteten Rufnummern.

11) Konfigurieren Sie jetzt die ISDN- und analogen Teilnehmer.

12) Ändern Sie die Einstellungen für eine MeetMe-Konferenz. Sie müssen eine eindeutige Kennzahl im Netzwerkverbund eingeben.

13) Konfigurieren Sie jetzt den E-Mail-Versand.

14) Klicken Sie auf **Beenden**.

20.6.10.6 Wie Sie die Vernetzung für Knoten 2 (Slave) konfigurieren

Im nächsten Schritt wird über den Wizard die Vernetzung von Knoten 2 konfiguriert.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Grundinstallation**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Vernetzung-Konfiguration** zu starten.

4) Wählen Sie die Einstellung **Netzwerk mit OSBiz X / OSBiz S**.

5) Aktivieren Sie unter **Knotentyp** das Kästchen **Dieses System ist ein SLAVE-Knoten**.

6) **Geben Sie die IP-Adresse des MASTER-Knotens ein** (Eine OpenScape Business wird als Slave-Knoten eingerichtet und die entsprechende IP-Adresse des Master-Knotens, der OpenScape Business S, eingetragen. Master und Multi-Gateway werden immer dem gleichen System, im Einrichtebeispiel der OpenScape Business S zugeordnet).

> ***INFO:*** Nach dem Klicken von **OK & Weiter** kann diese Aktion nicht mehr rückgängiggemacht werden!

7) Der **Registrierungsstatus** wird mit **Status erfolgreich** angezeigt (oder mit entsprechender Fehlermeldung). Damit ist der Wizard abgeschlossen.

8) Klicken Sie auf **Beenden**.

20.6.10.7 Wie Sie die Basisinstallation für Knoten 3 (Slave) konfigurieren

Für die Integration in einen Netzwerkverbund müssen die Ländervorwahl und eine Knoten-ID zugewiesen werden. Die internen Rufnummern müssen netzweit eindeutig konfiguriert werden. Die Eingabe der nationalen und lokalen Rufnummern ist wichtig, da diese Rufnummer in der Rtg1 ISDN Amt eingestellt wird und zur Normalisierung als Standortrufnummer verwendet wird.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Basisinstallation**.

3) Geben Sie im Feld **Ländervorwahl** die Ländervorwahl ein, z. B. 49 für Deutschland.

4) Tragen Sie die **Ortskennzahl** und **Anlagenrufnummer** ein.

5) Aktivieren Sie das Kontrollkästchen **Netzwerk-Integration**.

6) Vergeben Sie im Feld **Knoten-ID** für eine OpenScape Business eine im Netzverbund eindeutige Knoten-ID (eine "**3**" für das Einrichtebeispiel).

7) Klicken Sie auf **Funktion ausführen**. Sie werden zum Fenster **Zentrale Teilnehmer-Funktionen** geführt.

8) Da in einem Netzwerk alle internen Rufnummern eindeutig sein müssen, sind die Standard-Rufnummern zu löschen. Aktivieren Sie dazu das Optionsfeld **Alle Rufnummern löschen**.

9) Aktivieren Sie das Kontrollkästchen **Alle Rufnummern löschen** und klicken Sie auf **OK & Weiter**. Sie werden zum Fenster **Vorkonfigurierte Rufnummern ändern** geführt.

INFO: Die Funktionskennzahlen müssen im Netzwerkverbund eindeutig sein. Doppelte Rufnummern sind nicht zulässig!

---

10) Passen Sie die vorkonfigurierten Rufnummern an die Rufnummern im Netzwerk an und klicken Sie auf **OK & Weiter**. Die Rufnummern können Sie entweder manuell über den Wizard anpassen oder Sie importieren eine CSV-Datei mit den entsprechend vorbereiteten Rufnummern.

11) Konfigurieren Sie jetzt die ISDN- und analogen Teilnehmer.

12) Ändern Sie die Einstellungen für eine MeetMe-Konferenz. Sie müssen eine eindeutige Kennzahl im Netzwerkverbund eingeben.

13) Konfigurieren Sie jetzt den E-Mail-Versand.

14) Klicken Sie auf **Beenden**.

20.6.10.8 Wie Sie die Vernetzung für Knoten 3 (Slave) konfigurieren

Im nächsten Schritt wird über den Wizard für die Vernetzung von Knoten 3 konfiguriert.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Grundinstallation**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Vernetzung-Konfiguration** zu starten.

4) Wählen Sie die Einstellung **Netzwerk mit OSBiz X / OSBiz S**.

5) Aktivieren Sie unter **Knotentyp** das Kästchen **Dieses System ist ein SLAVE-Knoten**.

6) **Geben Sie die IP-Adresse des MASTER-Knotens ein** (Eine OpenScape Business wird als Slave-Knoten eingerichtet und die entsprechende IP-Adresse des Master-Knotens, der OpenScape Business S, eingetragen. Master und Multi-Location werden immer dem gleichen System, im Einrichtebeispiel der OpenScape Business S zugeordnet).

INFO: Nach dem Klicken von **OK & Weiter** kann diese Aktion nicht mehr rückgängiggemacht werden!

---

7) Der **Registrierungsstatus** wird mit **Status erfolgreich** angezeigt (oder mit entsprechender Fehlermeldung). Damit ist der Wizard abgeschlossen.

8) Klicken Sie auf **Beenden**.

20.6.10.9 Wie Sie die Vernetzungsfunktion für den Master kontrollieren

Sie können den Status der Vernetzung generell und die einzelnen Rufnummern kontrollieren.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Netzwerk**.

2) In der Statuszeile sehen Sie den **Synchronisationsstatus** für das Netzwerk. Grün bedeutet, dass die Vernetzung keine Probleme hat, Rot bedeutet Probleme im Netzwerk.

3) Markieren Sie im Fenster **Netzwerk** die Registerkarte **Knoten-Sicht** und es werden alle verfügbaren Knoten mit **Knoten ID**, **Name**, **System Typ**, **Server Adresse**, **Registrierungsstatus** und **Verfügbarkeitsstatus** angezeigt.

4) Markieren sie im Fenster **Netzwerk** die Registerkarte **Rufnummern** und es öffnet sich ein Fenster mit allen Angaben zu:

Rufnummer
DuWa
Name
Port Typ
Knoten

20.6.10.10 Wie Sie ein Multi-Gateway für Knoten 4 (Master) konfigurieren

Die Einrichtung des Netzwerverbunds als Multi-Gateway-Netzwerk wird am Master-Knoten vorgenommen.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Vernetzung-Konfiguration**.

3) Wählen Sie die unter **Netzwerk-Konfiguration** die Einstellung **Multi-Standort-Einrichtung**. Im Fenster **Multi-Standort-Einrichtung** wird die Zuordnung der Teilnehmer zum Standort festgelegt. Die Zuordnung der Rufnummer zur Knoten-ID (Node-ID) wird z. B. für die gehende Amtsbelegung im zugeordneten Standortknoten verwendet.

4) Geben Sie für das Einrichtebeispiel folgende Zuordnungen unter **Multi-Standort-Einrichtung** an (alle Telefone sind an OpenScape Business S registriert):

Rufnummer	Name	Node-ID
1101	1101KN1	1-Slave Witten1
1102	1102KN1	1-Slave Witten1
1103	1103KN1	1-Slave Witten1
2101	2101KN2	2-Slave Muenchen
2102	2102KN2	2-Slave Muenchen
2103	2103KN2	2-Slave Muenchen
3101	3101KN3	3-Slave Witten 2
3102	3102KN3	3-Slave Witten 2
3103	3103KN3	3-Slave Witten 2

5) Klicken Sie auf **Beenden**.

20.6.10.11 Wie Sie die Richtung und Richtungsparameter konfigurieren (Knoten 1, Slave)

Mit folgenden Schritten konfigurieren Sie die Richtung und die Richtungsparamter für die Vernetzung des Slaves.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Leitungen/Vernetzung**.

3) Klicken Sie im Menübaum auf **Richtung**.

4) Geben Sie im Fenster **Richtung ändern** im Feld **Richtungsname** einen Namen `Rtg. 1` für die Amtsrichtung ein.

5) Geben Sie unter **Richtungskennzahl** die `0` ein.

6) Geben Sie unter **Anlagenrufnummer-kommend** im Feld **Ländervorwahl** die `49` ein.

7) Geben Sie unter **Anlagenrufnummer-kommend** im Feld **Ortsnetzkennzahl** die `2302` ein.

8) Geben Sie unter **Anlagenrufnummer-kommend** im Feld **Anlagenrufnummer** die `66758` ein.

9) Markieren Sie das Kontrollkästchen unter **Anlagenrufnummer-kommend** im Feld **Standort-Nummer**.

10) Die Defaulte-Einstellungen für die Richtungsparameter (Nr.-Typ, gehen, Rufnummer Typ) können übernommen werden.

11) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

20.6.10.12 Wie Sie LCR für die Vernetzung konfigurieren (Knoten 1, Slave)

Im LCR-Wahlplan sind die Default-Einträge im Index 32, 33, 34 und 35 um weitere Einträge für die Wahl von Rufnummern im Format "International, National und Teilnehmer" zu den Knoten 2 und 3 sowie zum Multi-Gateway Knoten 4 zu ergänzen. "International" und "National" werden immer benötigt, "Teilnehmer" nur für Partnerknoten, die sich im gleichen Ortsnetz befinden.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > LCR**.

3) Klicken Sie im Menübaum auf **Wahlplan**.

4) Geben Sie folgende Werte auf freien Plätzen (hier 36 bis 43) nach den Standardwerten ein:

Wahlplan	Name	Gewählte Ziffern	Wegetabelle
31	Appl-Suite	-171	12
32	Standard	88CZ	1
33	IP-Network	-Z	13
34	COInternat	0C0049-Z	14
36	Knoten 2 Inter	0C004989722-Z	16
37	Knoten 2 Nat	0C089722-Z	16
38	Knoten 3 Inter	0C0049230266719-Z	17

Wahlplan	Name	Gewählte Ziffern	Wegetabelle
39	Knoten 3 Nat	0C0230266719-Z	17
40	Knoten 3 Teiln.	0C66719-Z	17
41	Knoten 4 Inter	0C0049230266758-Z	18
42	Knoten 4 Nat	0C0230266758-Z	18
43	Knoten 4 Teiln.	0C66758-Z	18
44			-

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

6) Klicken Sie im Menübaum auf die zugehörige **Wahlregel** für Knoten 2.

- ***a)*** Geben Sie unter **Regelname** den Eintrag **Knoten 2** ein.
- ***b)*** Geben Sie unter **Wahlregelformat** den Eintrag **D4989722E3A** ein.
- ***c)*** Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus.
- ***d)*** Wählen Sie unter **Type** den Eintrag **Ländervorwahl** aus.
- ***e)*** Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

7) Klicken Sie im Menübaum auf **Wegetabelle**, um die Wegetabelle 16 für das Networking zu konfigurieren und dem Knoten 2 direkt zuzuordnen.

- ***a)*** Klicken Sie auf die Wegetabelle 16.
- ***b)*** Wählen Sie unter **Richtung** den Eintrag **Networking** aus.
- ***c)*** Wählen Sie unter **Wahlregel** den Eintrag **Knoten 2** aus.
- ***d)*** Wählen Sie unter **Min. Ber.** den Eintrag **15** aus.
- ***e)*** Wählen Sie unter **Warnung** den Eintrag **Keine** aus.
- ***f)*** Wählen Sie unter **Dediziertes Gateway** den Eintrag **Erzwungen** aus.
- ***g)*** Wählen Sie unter **GW Knoten-ID** den Eintrag **2** aus.
- ***h)*** Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

8) Klicken Sie im Menübaum auf die zugehörige **Wahlregel** für Knoten 3.

- ***a)*** Geben Sie unter **Regelname** den Eintrag **Knoten 3** ein.
- ***b)*** Geben Sie unter **Wahlregelformat** den Eintrag **D49230266719E3A** ein.
- ***c)*** Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus.
- ***d)*** Wählen Sie unter **Type** den Eintrag **Ländervorwahl** aus.
- ***e)*** Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9) Klicken Sie im Menübaum auf **Wegetabelle**, um eine Wegetabelle 17 für das Networking zu konfigurieren und dem Knoten 3 direkt zuzuordnen.

- ***a)*** Klicken Sie auf die Wegetabelle 17.
- ***b)*** Wählen Sie unter **Richtung** den Eintrag **Networking** aus.

c) Wählen Sie unter **Wahlregel** den Eintrag **Knoten 3** aus.

d) Wählen Sie unter **Min. Ber.** den Eintrag **15** aus.

e) Wählen Sie unter **Warnung** den Eintrag **Keine** aus.

f) Wählen Sie unter **Dediziertes Gateway** den Eintrag **Erzwungen** aus.

g) Wählen Sie unter **GW Knoten-ID** den Eintrag **3** aus.

h) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10) Klicken Sie im Menübaum auf die zugehörige **Wahlregel** für Knoten 4.

a) Geben Sie unter **Regelname** den Eintrag **ML Knoten 4** ein.

b) Geben Sie unter **Wahlregelformat** den Eintrag **D230266758E3A** ein.

c) Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus.

d) Wählen Sie unter **Type** den Eintrag **National** aus.

e) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

11) Klicken Sie im Menübaum auf **Wegetabelle**, um eine Wegetabelle 18 für das Networking zu konfigurieren und dem Knoten 4 direkt zuzuordnen.

a) Klicken Sie auf die Wegetabelle 18.

b) Wählen Sie unter **Richtung** den Eintrag **Networking** aus.

c) Wählen Sie unter **Wahlregel** den Eintrag **Knoten 4** aus.

d) Wählen Sie unter **Min. Ber.** den Eintrag **15** aus.

e) Wählen Sie unter **Warnung** den Eintrag **Keine** aus.

f) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

20.6.10.13 Wie Sie die Richtung und Richtungsparameter konfigurieren (Knoten 2, Slave)

Mit folgenden Schritten konfigurieren Sie die Richtung und die Richtungsparamter für die Vernetzung des Slaves.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Leitungen/Vernetzung**.

3) Klicken Sie im Menübaum auf **Richtung**.

4) Geben Sie im Fenster **Richtung ändern** im Feld **Richtungsname** einen Namen `Rtg. 1` für die Amtsrichtung ein.

5) Geben Sie unter **Richtungskennzahl** die `0` ein.

6) Geben Sie unter **Anlagenrufnummer-kommend** im Feld **Ländervorwahl** die `49` ein.

7) Geben Sie unter **Anlagenrufnummer-kommend** im Feld **Ortsnetzkennzahl** die 89 ein.

8) Geben Sie unter **Anlagenrufnummer-kommend** im Feld **Anlagenrufnummer** die `722` ein.

9) Markieren Sie das Kontrollkästchen unter **Anlagenrufnummer-kommend** im Feld **Standort-Nummer**.

10) Die Defaulte-Einstellungen für die Richtungsparameter (Nr.-Typ, gehen, Rufnummer Typ) können übernommen werden.

11) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

20.6.10.14 Wie Sie LCR für die Vernetzung konfigurieren (Knoten 2, Slave)

Im LCR Wahlplan sind die Default-Einträge im Index 32, 33, 34 und 35 um weitere Einträge für die Wahl von Rufnummern im Format "International, National und Teilnehmer" zu den Knoten 1 und 2 zu ergänzen. "International" und "National" werden immer benötigt, "Teilnehmer" nur für Partnerknoten, die sich im gleichen Ortsnetz befinden. Die Einträge 36, 37 und 38 für das Interworking mit Knoten 1 (Rufnummer 100 > 199) und die Einträge 39, 40 und 41 für das Interworking mit Knoten 3 (Rufnummer 300 > 399) sind zu ergänzen. Diese Angaben werden für die Wahl aus Applikationen (z. B. myPortal for Desktop) verwendet.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > LCR**.

3) Klicken Sie im Menübaum auf **Wahlplan**.

4) Geben Sie folgende Werte auf freien Plätzen (hier 36 bis 43) nach den Standardwerten ein:

Wahlplan	Name	Gewählte Ziffern	Wegetabelle
31	Appl-Suite	-171	12
32	Standard	88CZ	1
33	IP-Network	-Z	13
34	COInternat	0C0049-Z	14
36	Knoten 1 Inter	0C0049230266758-Z	16
37	Knoten 1 Nat	0C0230266758-Z	16

Wahlplan	Name	Gewählte Ziffern	Wegetabelle
38	Knoten 3 Inter	0C0049230266719-Z	17
39	Knoten 3 Nat	0C0230266719-Z	17
40	Knoten 3 Teiln.	0C66719-Z	17
41	Knoten 4 Inter	0C004989722-Z	18
42	Knoten 4 Nat	0C089722-Z	18
43	Knoten 4 Teiln.	0C722-Z	18
44			-

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

6) Klicken Sie im Menübaum auf die zugehörige **Wahlregel** für Knoten 1.

- ***a)*** Geben Sie unter **Regelname** den Eintrag **Knoten 1** ein.
- ***b)*** Geben Sie unter **Wahlregelformat** den Eintrag **D49230266758E3A** ein.
- ***c)*** Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus.
- ***d)*** Wählen Sie unter **Type** den Eintrag **Ländervorwahl** aus.
- ***e)*** Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

7) Klicken Sie im Menübaum auf **Wegetabelle**, um die Wegetabelle 16 für das Networking zu konfigurieren und dem Knoten 1 direkt zuzuordnen.

- ***a)*** Klicken Sie auf die Wegetabelle 16.
- ***b)*** Wählen Sie unter **Richtung** den Eintrag **Networking** aus.
- ***c)*** Wählen Sie unter **Wahlregel** den Eintrag **Knoten 1** aus.
- ***d)*** Wählen Sie unter **Min. Ber.** den Eintrag **15** aus.
- ***e)*** Wählen Sie unter **Warnung** den Eintrag **Keine** aus.
- ***f)*** Wählen Sie unter **Dediziertes Gateway** den Eintrag **Erzwungen** aus.
- ***g)*** Wählen Sie unter **GW Knoten-ID** den Eintrag **1** aus.
- ***h)*** Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

8) Klicken Sie im Menübaum auf die zugehörige **Wahlregel** für Knoten 3.

- ***a)*** Geben Sie unter **Regelname** den Eintrag **Knoten 3** ein.
- ***b)*** Geben Sie unter **Wahlregelformat** den Eintrag **D49230266719E3A** ein.
- ***c)*** Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus.
- ***d)*** Wählen Sie unter **Type** den Eintrag **Ländervorwahl** aus.
- ***e)*** Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9) Klicken Sie im Menübaum auf **Wegetabelle**, um eine Wegetabelle 17 für das Networking zu konfigurieren und dem Knoten 3 direkt zuzuordnen.

- ***a)*** Klicken Sie auf die Wegetabelle 17.

b) Wählen Sie unter **Richtung** den Eintrag **Networking** aus.

c) Wählen Sie unter **Wahlregel** den Eintrag **Knoten 3 direkt** aus.

d) Wählen Sie unter **Min. Ber.** den Eintrag **15** aus.

e) Wählen Sie unter **Warnung** den Eintrag **Keine** aus.

f) Wählen Sie unter **Dediziertes Gateway** den Eintrag **Erzwungen** aus.

g) Wählen Sie unter **GW Knoten-ID** den Eintrag **3** aus.

h) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10) Klicken Sie im Menübaum auf die zugehörige **Wahlregel** für Knoten 4.

a) Geben Sie unter **Regelname** den Eintrag **Knoten 4** ein.

b) Geben Sie unter **Wahlregelformat** den Eintrag **D89722E3A** ein.

c) Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus.

d) Wählen Sie unter **Type** den Eintrag **Ortsnetzkennzahl** aus.

e) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

11) Klicken Sie im Menübaum auf **Wegetabelle**, um eine Wegetabelle 18 für das Networking zu konfigurieren und dem Knoten 4 direkt zuzuordnen.

a) Klicken Sie auf die Wegetabelle 18.

b) Wählen Sie unter **Richtung** den Eintrag **Networking** aus.

c) Wählen Sie unter **Wahlregel** den Eintrag **Knoten 4** aus.

d) Wählen Sie unter **Min. Ber.** den Eintrag **15** aus.

e) Wählen Sie unter **Warnung** den Eintrag **Keine** aus.

f) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

20.6.10.15 Wie Sie die Richtung und Richtungsparameter konfigurieren (Knoten 3, Slave)

Mit folgenden Schritten konfigurieren Sie die Richtung und die Richtungsparamter für die Vernetzung des Slaves.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Leitungen/Vernetzung**.

3) Klicken Sie im Menübaum auf **Richtung**.

4) Geben Sie im Fenster **Richtung ändern** im Feld **Richtungsname** einen Namen `Rtg. 1` für die Amtsrichtung ein.

5) Geben Sie unter **Richtungskennzahl** die `0` ein.

6) Geben Sie unter **Anlagenrufnummer-kommend** im Feld **Ländervorwahl** die `49` ein.

7) Geben Sie unter **Anlagenrufnummer-kommend** im Feld **Ortsnetzkennzahl** die `2302` ein.

8) Geben Sie unter **Anlagenrufnummer-kommend** im Feld **Anlagenrufnummer** die `66719` ein.

9) Markieren Sie das Kontrollkästchen unter **Anlagenrufnummer-kommend** im Feld **Standort-Nummer**.

10) Die Defaulte-Einstellungen für die Richtungsparameter (Nr.-Typ, gehen, Rufnummer Typ) können übernommen werden.

11) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

20.6.10.16 Wie Sie LCR für die Vernetzung konfigurieren (Knoten 3, Slave)

Im LCR Wahlplan sind die Default-Einträge im Index 32, 33, 34 und 35 um weitere Einträge für die Wahl von Rufnummern im Format "International, National und Teilnehmer" zu den Knoten 1 und 2 zu ergänzen. "International" und "National" werden immer benötigt, "Teilnehmer" nur für Partnerknoten, die sich im gleichen Ortsnetz befinden. Diese Angaben werden für die Wahl aus Applikationen (z. B. myPortal for Desktop) verwendet.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > LCR**.

3) Klicken Sie im Menübaum auf **Wahlplan**.

4) Geben Sie folgende Werte ein:

Wahlplan	Name	Gewählte Ziffern	Wegetabelle
31	Appl-Suite	-171	12
32	Standard	88CZ	1
33	IP-Network	-Z	13
34	COInternat	0C0049-Z	14
36	Knoten 1 Inter	0C0049230266758-Z	16
37	Knoten 1 Nat	0C00230266758-Z	16
38	Knoten 1 Teiln.	0C66758-Z	16

Wahlplan	Name	Gewählte Ziffern	Wegetabelle
39	Knoten 2 Inter	0C004989722-Z	17
40	Knoten 2 Nat	0C0089722-Z	17
41	Knoten 4 Inter	0C0049230266719-Z	18
42	Knoten 4 Nat	0C0230266719-Z	18
43	Knoten 4 Teiln.	0C66719-Z	18
44			-

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

6) Klicken Sie im Menübaum auf die zugehörige **Wahlregel** für Knoten 1.

- ***a)*** Geben Sie unter **Regelname** den Eintrag **Knoten 1** ein.
- ***b)*** Geben Sie unter **Wahlregelformat** den Eintrag **D49230266758E3A** ein.
- ***c)*** Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus.
- ***d)*** Wählen Sie unter **Type** den Eintrag **Ländervorwahl** aus.
- ***e)*** Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

7) Klicken Sie im Menübaum auf **Wegetabelle**, um die Wegetabelle 16 für das Networking zu konfigurieren und dem Knoten 1 direkt zuzuordnen.

- ***a)*** Klicken Sie auf die Wegetabelle 16.
- ***b)*** Wählen Sie unter **Richtung** den Eintrag **Networking** aus.
- ***c)*** Wählen Sie unter **Wahlregel** den Eintrag **Knoten 1** aus.
- ***d)*** Wählen Sie unter **Min. Ber.** den Eintrag **15** aus.
- ***e)*** Wählen Sie unter **Warnung** den Eintrag **Keine** aus.
- ***f)*** Wählen Sie unter **Dediziertes Gateway** den Eintrag **Erzwungen** aus.
- ***g)*** Wählen Sie unter **GW Knoten-ID** den Eintrag **1** aus.
- ***h)*** Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

8) Klicken Sie im Menübaum auf die zugehörige **Wahlregel** für Knoten 2.

- ***a)*** Geben Sie unter **Regelname** den Eintrag **Knoten 2** ein.
- ***b)*** Geben Sie unter **Wahlregelformat** den Eintrag **D4989722E3A** ein.
- ***c)*** Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus.
- ***d)*** Wählen Sie unter **Type** den Eintrag **Ländervorwahl** aus.
- ***e)*** Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9) Klicken Sie im Menübaum auf **Wegetabelle**, um eine Wegetabelle 17 für das Networking zu konfigurieren und dem Knoten 2 direkt zuzuordnen.

- ***a)*** Klicken Sie auf die Wegetabelle 17.
- ***b)*** Wählen Sie unter **Richtung** den Eintrag **Networking** aus.

c) Wählen Sie unter **Wahlregel** den Eintrag **Knoten 2** aus.

d) Wählen Sie unter **Min. Ber.** den Eintrag **15** aus.

e) Wählen Sie unter **Warnung** den Eintrag **Keine** aus.

f) Wählen Sie unter **Dediziertes Gateway** den Eintrag **Erzwungen** aus.

g) Wählen Sie unter **GW Knoten-ID** den Eintrag **2** aus.

h) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10) Klicken Sie im Menübaum auf die zugehörige **Wahlregel** für Knoten 4.

a) Geben Sie unter **Regelname** den Eintrag **ML Knoten 4** ein

b) Geben Sie unter **Wahlregelformat** den Eintrag **D230266719E3A** ein

c) Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus

d) Wählen Sie unter **Type** den Eintrag **Ortsnetzkennzahl** aus

e) Klicken Sie auf **Übernehmen** und anschließend auf **OK**

11) Klicken Sie im Menübaum auf **Wegetabelle**, um eine Wegetabelle 18 für das Networking zu konfigurieren und dem Knoten 4 direkt zuzuordnen.

a) Klicken Sie auf die Wegetabelle 18.

b) Wählen Sie unter **Richtung** den Eintrag **Networking** aus.

c) Wählen Sie unter **Wahlregel** den Eintrag **Knoten 4** aus.

d) Wählen Sie unter **Min. Ber.** den Eintrag **15** aus.

e) Wählen Sie unter **Warnung** den Eintrag **Keine** aus.

f) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

20.6.10.17 Wie Sie die Richtung und Richtungsparameter konfigurieren (Knoten 4, Master)

Mit folgenden Schritten konfigurieren Sie die Richtung und die Richtungsparameter für die Vernetzung der Slaves.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Leitungen/Vernetzung**.

3) Klicken Sie im Menübaum auf **Richtung**.

4) Geben Sie im Fenster **Richtung ändern** im Feld **Richtungsname** einen Namen `Rtg. 1` für die Amtsrichtung ein.

5) Geben Sie unter **Richtungskennzahl** die `0` ein.

6) Geben Sie unter **Anlagenrufnummer-kommend** im Feld **Ländervorwahl** die `49` ein.

7) Machen Sie keine Eintragungen in den Feldern **Ortsnetzkennzahl** und Anlagenrufnummer.

8) Markieren Sie das Kontrollkästchen unter **Anlagenrufnummer-kommend** im Feld **Standort-Nummer**.

9) Die Default-Einstellungen für die Richtungsparameter (Nr.-Typ, gehen, Rufnummer Typ) können übernommen werden.

10) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

20.6.10.18 Wie Sie LCR für die Vernetzung konfigurieren (Knoten 4, Master)

Im LCR Wahlplan sind die Default-Einträge im Index 32, 33, 34 und 35 um weitere Einträge für die Wahl von Rufnummern im Format "International, National und Teilnehmer" zu den Knoten 1 und 2 zu ergänzen. "International" und "National" werden immer benötigt, "Teilnehmer" nur für Partnerknoten, die sich im gleichen Ortsnetz befinden. Diese Angaben werden für die Wahl aus Applikationen (z. B. myPortal for Desktop) verwendet.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > LCR**.

3) Klicken Sie im Menübaum auf **Wahlplan**.

4) Geben Sie folgende Werte auf freien Plätzen (hier 36 bis 43) nach den Standardwerten ein:

Wahlplan	Name	Gewählte Ziffern	Wegetabelle
1	Notruf	0C112	19
2	Notruf	0C110	19
3	Teleworking	0C0137Z	19
4	Televoting	0C0138Z	19
5	Premium Dienste	0C0900Z	19
6	Auskunftsdienst	0C118Z	19
7	Sonderrufnummer	0C116116	19
16	Standard	0CZ	19
17	Standard	0C1Z	19

Wahlplan	Name	Gewählte Ziffern	Wegetabelle
18	Standard	0CNZ	19
31	Appl-Suite	-471	12
32	Standard	88CZ	1
33	IP-Network	-Z	13
34	COInternat	0C0049-Z	15
36	Knoten 1 Inter	0C0049230266758-Z	16
37	Knoten 1 Nat	0C0230266758-Z	16
38	Knoten 1 Teiln.	0C66758-Z	16
39	Knoten 2 Inter	0C004989722-Z	17
40	Knoten 2 Nat	0C089722-Z	17
41	Knoten 3 Inter	0C0049230266719-Z	18
42	Knoten 3 Nat	0C0230266719-Z	18
43	Knoten 3 Teiln.	0C66719-Z	18
44			-

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

6) Klicken Sie im Menübaum auf die zugehörige **Wahlregel** für Knoten 1.

- ***a)*** Geben Sie unter **Regelname** den Eintrag **Knoten 1** ein.
- ***b)*** Geben Sie unter **Wahlregelformat** den Eintrag **D49230266758E3A** ein.
- ***c)*** Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus.
- ***d)*** Wählen Sie unter **Type** den Eintrag **Ländervorwahl** aus.
- ***e)*** Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

7) Klicken Sie im Menübaum auf **Wegetabelle**, um die Wegetabelle 16 für das Networking zu konfigurieren und dem Knoten 1 direkt zuzuordnen.

- ***a)*** Klicken Sie auf die Wegetabelle 16.
- ***b)*** Wählen Sie unter **Richtung** den Eintrag **Networking** aus.
- ***c)*** Wählen Sie unter **Wahlregel** den Eintrag **Knoten 1** aus.
- ***d)*** Wählen Sie unter **Min. Ber.** den Eintrag **15** aus.
- ***e)*** Wählen Sie unter **Warnung** den Eintrag **Keine** aus.
- ***f)*** Wählen Sie unter **Dediziertes Gateway** den Eintrag **Erzwungen** aus.
- ***g)*** Wählen Sie unter **GW Knoten-ID** den Eintrag **1** aus.
- ***h)*** Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

8) Klicken Sie im Menübaum auf die zugehörige **Wahlregel** für Knoten 2.

- ***a)*** Geben Sie unter **Regelname** den Eintrag **Knoten 2** ein.
- ***b)*** Geben Sie unter **Wahlregelformat** den Eintrag **D4989722E3A** ein.

c) Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus.

d) Wählen Sie unter **Type** den Eintrag **Ländervorwahl** aus.

e) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

9) Klicken Sie im Menübaum auf **Wegetabelle**, um eine Wegetabelle 17 für das Networking zu konfigurieren und dem Knoten 2 direkt zuzuordnen.

a) Klicken Sie auf die Wegetabelle 17.

b) Wählen Sie unter **Richtung** den Eintrag **Networking** aus.

c) Wählen Sie unter **Wahlregel** den Eintrag **Knoten 2** aus.

d) Wählen Sie unter **Min. Ber.** den Eintrag **15** aus.

e) Wählen Sie unter **Warnung** den Eintrag **Keine** aus.

f) Wählen Sie unter **Dediziertes Gateway** den Eintrag **Erzwungen** aus.

g) Wählen Sie unter **GW Knoten-ID** den Eintrag **2** aus.

h) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

10) Klicken Sie im Menübaum auf die zugehörige **Wahlregel** für Knoten 3.

a) Geben Sie unter **Regelname** den Eintrag **ML Knoten 3** ein

b) Geben Sie unter **Wahlregelformat** den Eintrag **D230266719E3A** ein

c) Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus

d) Wählen Sie unter **Type** den Eintrag **Ländervorwahl** aus

e) Klicken Sie auf **Übernehmen** und anschließend auf **OK**

11) Klicken Sie im Menübaum auf **Wegetabelle**, um eine Wegetabelle 18 für das Networking zu konfigurieren und dem Knoten 3 direkt zuzuordnen.

a) Klicken Sie auf die Wegetabelle 18.

b) Wählen Sie unter **Richtung** den Eintrag **Networking** aus.

c) Wählen Sie unter **Wahlregel** den Eintrag **Knoten 3** aus.

d) Wählen Sie unter **Min. Ber.** den Eintrag **15** aus.

e) Wählen Sie unter **Warnung** den Eintrag **Keine** aus.

f) Wählen Sie unter **Dediziertes Gateway** den Eintrag **Erzwungen** aus.

g) Wählen Sie unter **GW Knoten-ID** den Eintrag **3** aus.

h) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

12) Klicken Sie im Menübaum auf die zugehörige **Wahlregel** für Amtsgespräche. Es handelt sich um die vordefinierte Wahlregel "Gateway Call".

a) Geben Sie unter **Regelname** den Eintrag **Gateway Call** ein.

b) Geben Sie unter **Wahlregelformat** den Eintrag **E1A** ein.

c) Wählen Sie unter **Verfahren des Netzanbieters** den Eintrag **Corporate Network** aus.

d) Wählen Sie unter **Type** den Eintrag **Unbekannt** aus.

e) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

13) Klicken Sie im Menübaum auf **Wegetabelle**, um die Wegetabelle 19 für den Amtsausstieg der Slaves zu konfigurieren. Anhand der Eintragung Multi-Gateway wird die Zugehörigkeit des Teilnehmers zum Knoten bestimmt und an diesem Knoten der Amtsausstieg vorgenommen.

14) Klicken Sie auf die Wegetabelle 19.

a) Wählen Sie unter **Richtung** den Eintrag **Networking** aus.

b) Wählen Sie unter **Wahlregel** den Eintrag **Gateway Call** aus.

c) Wählen Sie unter **Min. Ber.** den Eintrag **15** aus.

d) Wählen Sie unter **Warnung** den Eintrag **Keine** aus.

e) Wählen Sie unter **Dediziertes Gateway** den Eintrag **Multi-Gateway** aus.

f) Wählen Sie unter **GW Knoten-ID** den Eintrag **1** aus.

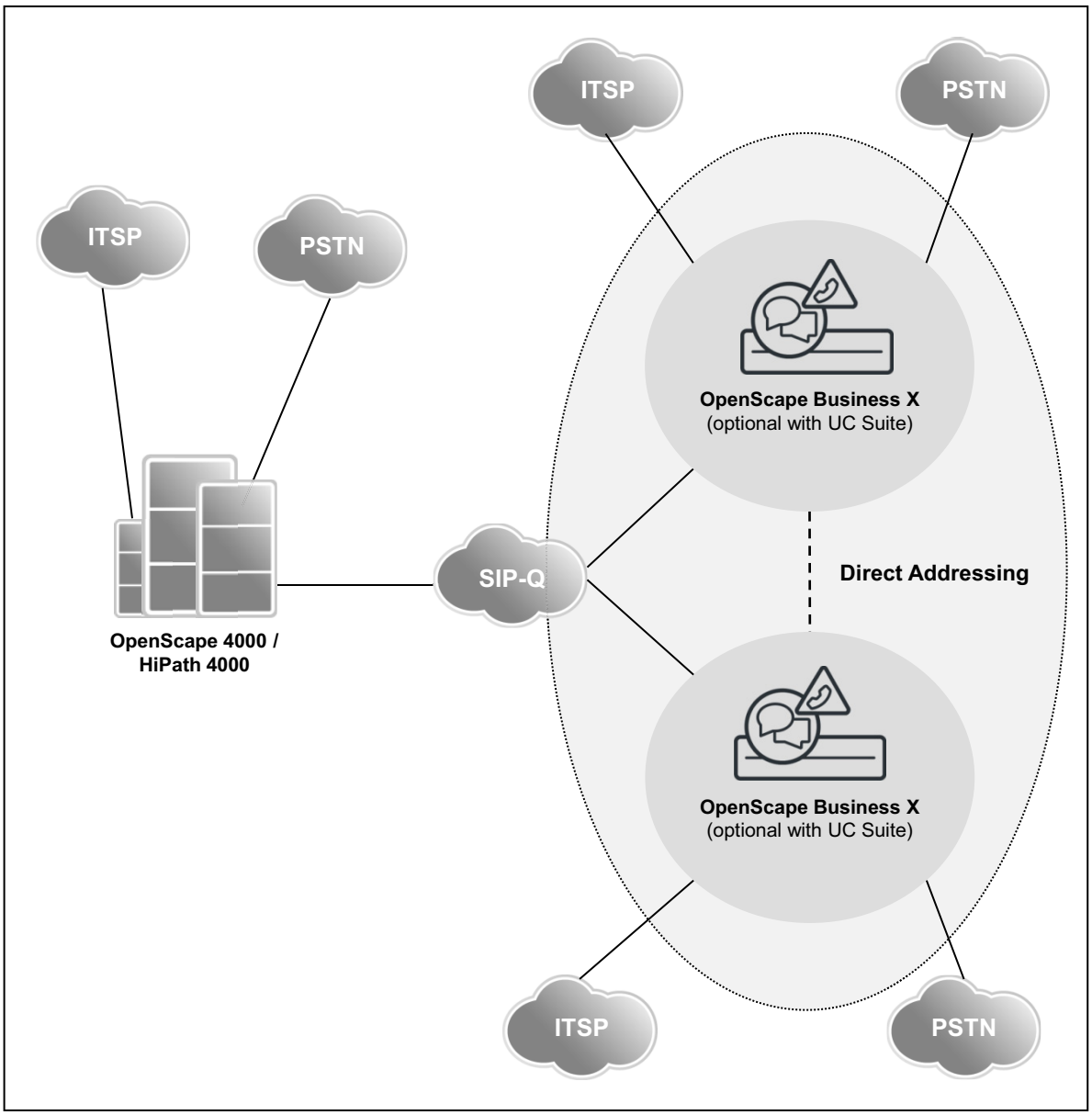
g) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

20.6.11 Szenario 4: Vernetzung von OpenScape Business X und OpenScape 4000/HiPath 4000

Eine Vernetzung von OpenScape Business X mit OpenScape 4000/HiPath 4000 kann zwei unterschiedliche Ausprägungen haben. Erstens mit direkter Adressierung zwischen den OpenScape Business Knoten (Szenario 4a) und zweitens mit Routing aller Verbindungen über OpenScape 4000/HiPath 4000 (Szenario 4b).

INFO: Ein Einrichtebeispiel zur Vernetzung mit OpenScape 4000/ HiPath 4000 finden Sie im Unify Experts Wiki unter `http://wiki.unify.com/wiki/How_to_collection_and_tutorials_for_OpenScape_Business`

Szenario 4a: Netzverbund mit OpenScape 4000/HiPath 4000 und direkter Adressierung zwischen den OpenScape Business X Knoten

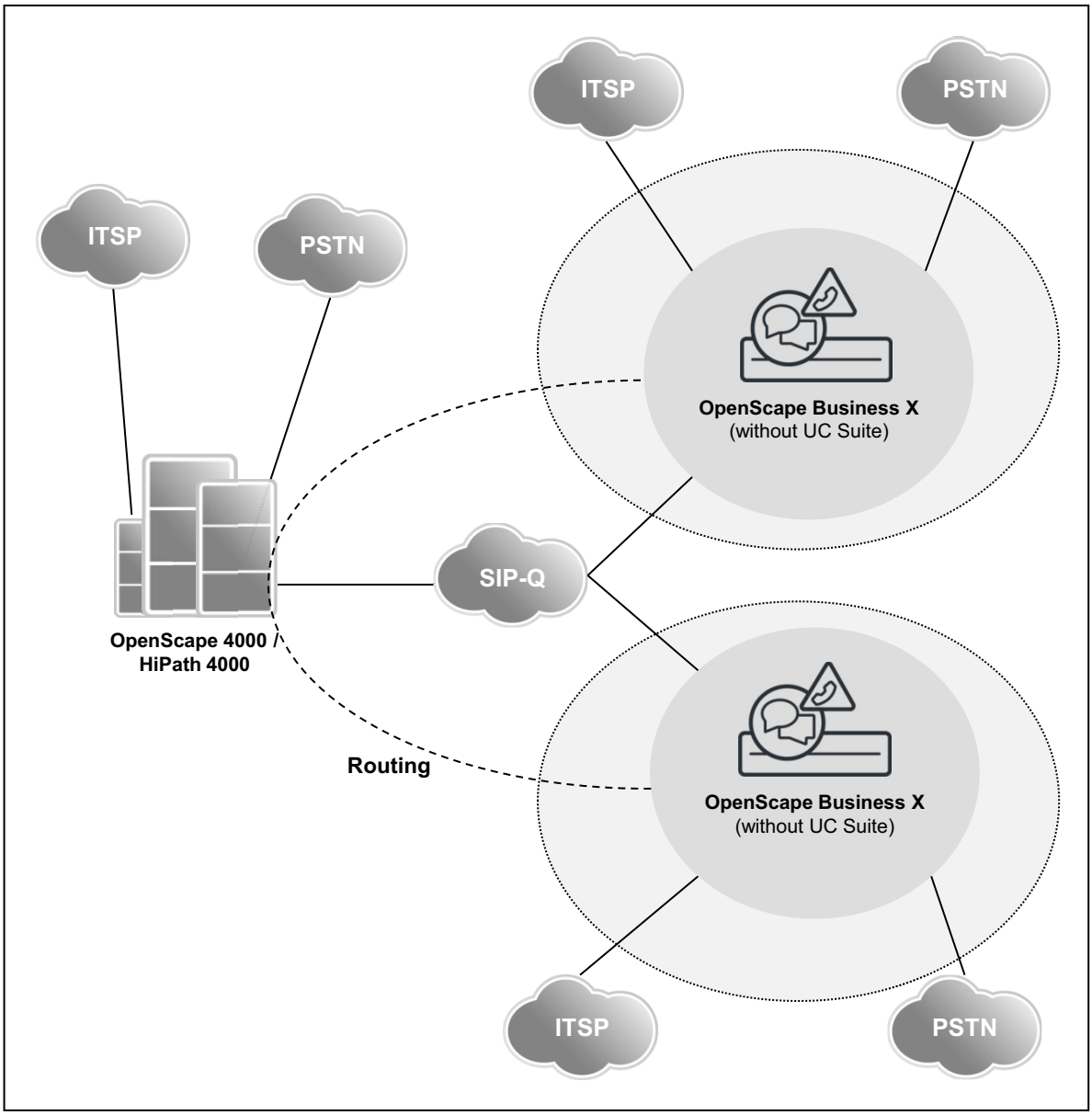


Netzwerkdaten:

- Geschlossene Nummerierung innerhalb der OpenScape Business Vernetzung
- Netztweite Sprach- und UC-Funktionalität innerhalb der OpenScape Business Vernetzung (UC Suite)
- Konfiguration über den Wizard Vernetzung für die OpenScape Business Vernetzung
- Konfiguration der OpenScape 4000/HiPath 4000 Netzanteile im Expertenmodus

- Small Remote Site Konzept SRS wird nicht unterstützt
- UC-Funktionalität über UC Booster Server oder über UC Booster Card ist optional.
- OpenScape Business S kann im Single oder Multi Gateway Modus integriert werden.

Szenario 4b: Netzverbund mit OpenScape 4000/HiPath 4000 und Routing aller Verbindungen über OpenScape 4000/HiPath 4000



Netzwerkdaten

- Offene Nummerierung
- Netzweite Sprach-Funktionalität

- Jedes Gespräch in einen anderen Knoten wird über OpenScape 4000/ HiPath 4000 geroutet
- Keine UC-Suite bei OpenScape Business wegen offener Nummerierung im Netzverbund
- Small Remote Site Konzept SRS wird nicht unterstützt
- Die Konfiguration muss für jeden Knoten im Expertenmodus erfolgen
- OpenScape Business S ist nicht in Netzen mit OpenScape 4000/HiPath 4000 und offener Nummerierung erlaubt, da in OpenScape Business S die UC Suite immer integriert ist.

20.6.12 Szenario 4: Netzweite Leistungsmerkmale

Ausbau	Geschlossene Nummerierung innerhalb der OpenScape Business Vernetzung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
Maximale Anzahl Knoten	100 (32 freigegeben, abhängig von OpenScape 4000/HiPath 4000)	
Maximale Anzahl von Teilnehmern pro System	abhängig vom OpenScape Business X Modell	
Maximale Anzahl von Teilnehmern im Netz	2000 (1000 freigegeben) für den OpenScape Business Netz-Anteil	abhängig von OpenScape 4000/ HiPath 4000
Sprachvernetzung	SIP-Q	

UC Vernetzung	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
	Netzweite Funktionalität innerhalb der OpenScape Business	Wird nicht unterstützt
UC Booster Server	Wird unterstützt	Wird nicht unterstützt
UC Booster Card	Wird unterstützt	Wird nicht unterstützt
OpenScape Business S	Wird unterstützt	Wird nicht unterstützt

Administration	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
	WBM mit Wizards für OpenScape Business Knoten, OpenScape 4000/ HiPath 4000 wird über Expertenmodus der OpenScape Business administriert	Netzweite Administration Expertenmodus
WBM	WBM mit Wizards	WBM mit Expertenmodus
Manager E	Nicht empfohlen	Nicht empfohlen
UC-Suite-Administration	WBM mit Wizards für OpenScape Business Knoten	Wird nicht unterstützt
Massendatenimport über csv-Dateien (Rufnummern, Durchwahlnummern, Namen)	Separat für jeden Knoten im Netzverbund	

Lizenzierung	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
Neue Lizenzierungsstruktur	Eine Vernetzungslizenz für jede OpenScape Business erforderlich	

myPortal for Desktop / myPortal for Outlook (UC Suite)	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
	Netzweit mit UC-Funktionalität über UC Booster Server, UC Booster Card oder OpenScape Business S	Wird nicht unterstützt
Instant Messaging	Netzweit, innerhalb der OpenScape Business Vernetzung	Wird nicht unterstützt
VoiceMail	Die Teilnehmer nutzer ihr lokales VoiceMail-System; es gibt keine zentrale VoiceMail für den gesamten Netzverbund.	Wird nicht unterstützt
Anwesenheitsstatus	Netzweit, innerhalb der OpenScape Business Vernetzung	Wird nicht unterstützt
Besetztanzeige	Netzweit, innerhalb der OpenScape Business Vernetzung	Wird nicht unterstützt
Internes Verzeichnis / Favoriten	Netzweit, innerhalb der OpenScape Business Vernetzung	Wird nicht unterstützt
Externes Verzeichnis	Lokal über den Import von csv-Dateien	Wird nicht unterstützt
Suche in externen Verzeichnissen anderer Knoten	Nicht möglich	Wird nicht unterstützt
Externes Offline-Verzeichnis (LDAP)	über LDAP	Wird nicht unterstützt

myPortal Smart (UC Smart)	Geschlossene Nummerierung	Offene Nummerierung
	Netzweit	Wird nicht unterstützt
VoiceMail	Die Teilnehmer nutzer ihr lokales VoiceMail-System; es gibt keine zentrale VoiceMail für den gesamten Netzverbund.	Wird nicht unterstützt
Anwesenheitsstatus	Lokal	Wird nicht unterstützt
Besetztanzeige	Lokal	Wird nicht unterstützt
Internes Verzeichnis / Favoriten	Lokal	Wird nicht unterstützt

myAttendant	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
	Mit UC-Funktionalität über UC Booster Server, UC Booster Card oder OpenScape Business S	Wird nicht unterstützt
Instant Messaging	Netzweit, innerhalb der OpenScape Business Vernetzung	Wird nicht unterstützt
VoiceMail	Die Teilnehmer nutzer ihr lokales VoiceMail-System; es gibt keine zentrale VoiceMail für den gesamten Netzverbund.	Wird nicht unterstützt
Anwesenheitsstatus	Netzweit, innerhalb der OpenScape Business Vernetzung	Wird nicht unterstützt
Besetztanzeige	Netzweit, innerhalb der OpenScape Business Vernetzung	Wird nicht unterstützt
Internes Verzeichnis / Favoriten	Netzweit, innerhalb der OpenScape Business Vernetzung	Wird nicht unterstützt
Externes Verzeichnis	Lokal über den Import von csv-Dateien	Wird nicht unterstützt
Suche in externen Verzeichnissen anderer Knoten	Nicht möglich	Wird nicht unterstützt
Externes Offline-Verzeichnis (LDAP)	über LDAP	Wird nicht unterstützt

OpenScape Business Attendant	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
	Schnittstelle beschränkt auf 8-stellige Rufnummern	Schnittstelle beschränkt auf 8-stellige Rufnummern
Anwesenheitsstatus	Netzweit, innerhalb der OpenScape Business Vernetzung über den BLF-Server	
Besetztanzeige	Netzweit, innerhalb der OpenScape Business Vernetzung über den BLF-Server	
Externes Verzeichnis	über LDAP	über LDAP
Zentraler Vermittlungsplatz	Netzweit, innerhalb der OpenScape Business Vernetzung	

Company AutoAttendant (UCSuite)	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
Company AutoAttendant: Nachdem der Auto-Attendant einen Anruf beantwortet hat, muss der Anrufer die Rufnummer wählen mit der er verbunden werden möchte.	ccv-Scripts erlauben es Rufnummern aus dem internen Verzeichnis innerhalb des Netzverbunds zu wählen.	Wird nicht unterstützt
Persönlicher AutoAttendant: Nachdem der AutoAttendant einen Anruf beantwortet hat, muss der Anrufer eine einstellige Ziffer wählen um mit seinem Anrufziel verbunden zu werden.	Jede von einem UC Teilnehmer vorkonfigurierte Rufnummer möglich	Wird nicht unterstützt

Company AutoAttendant (UC Smart)	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
Company AutoAttendant (UC Smart)	Lokal	Lokal

myAgent	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
	Mit UC-Funktionalität über UC Booster Server, UC Booster Card oder OpenScape Business S. Alle Agenten sind an EINEM Knoten registriert. Eingehend CC-Anrufe über das lokale PSTN, ITSP und SIP-Q-Amtssätze.	Wird nicht unterstützt
VoiceMail (Aufnahme, Message Waiting Indication, Abfrage)	Die Teilnehmer nutzer ihr lokales VoiceMail-System; es gibt keine zentrale VoiceMail für den gesamten Netzverbund	Wird nicht unterstützt
Anwesenheitsstatus	Netzweit	Wird nicht unterstützt
Besetztanzeige	Netzweit	Wird nicht unterstützt
Agentenstatus	Lokal	Wird nicht unterstützt
Internes Verzeichnis / Favoriten	Netzweit	Wird nicht unterstützt
Externes Verzeichnis	Lokal über Import von csv-Dateien	Wird nicht unterstützt
Suche in externen Verzeichnissen anderer Knoten	Nicht möglich	Wird nicht unterstützt
Externes Offline-Verzeichnis (LDAP)	Lokal	Wird nicht unterstützt
Übergabe eines Anrufs	Lokal	Wird nicht unterstützt
Kundeninformation	Lokal	Wird nicht unterstützt
Reporting	Lokal	Wird nicht unterstützt

Externe Applikationen	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
OpenScape Business TAPI-Applikation	Siehe *Application Connectivity*	
Externe CSTA-Applikationen		
Application Launcher		
OpenScape Contact Center	Siehe *Multimedia Contact Center*.	

Telefonie	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
SIP-Provider (ITSP)	Lokal	Lokal
PSTN-Provider	Lokal; Netzknoten ohne eigenen PSTN-Provider werden über SIP-Q bzw. das zugehörige Gateway erreicht.	
Survivability (Ausfallsicherheit im Falle eines Zusammenbruchs des Netzverbundes bzw. der OpenScape Business S)	Wird unterstützt zwischen OpenScape Business X und OpenScape Business S	Wird nicht unterstützt
Wahl einer öffentlichen Rufnummer im eigenen Knotens	Wird unterstützt	
Wahl einer öffentlichen Rufnummer in einem vernetzten Knotens	Netzweit innerhalb der OpenScape Business Vernetzung	

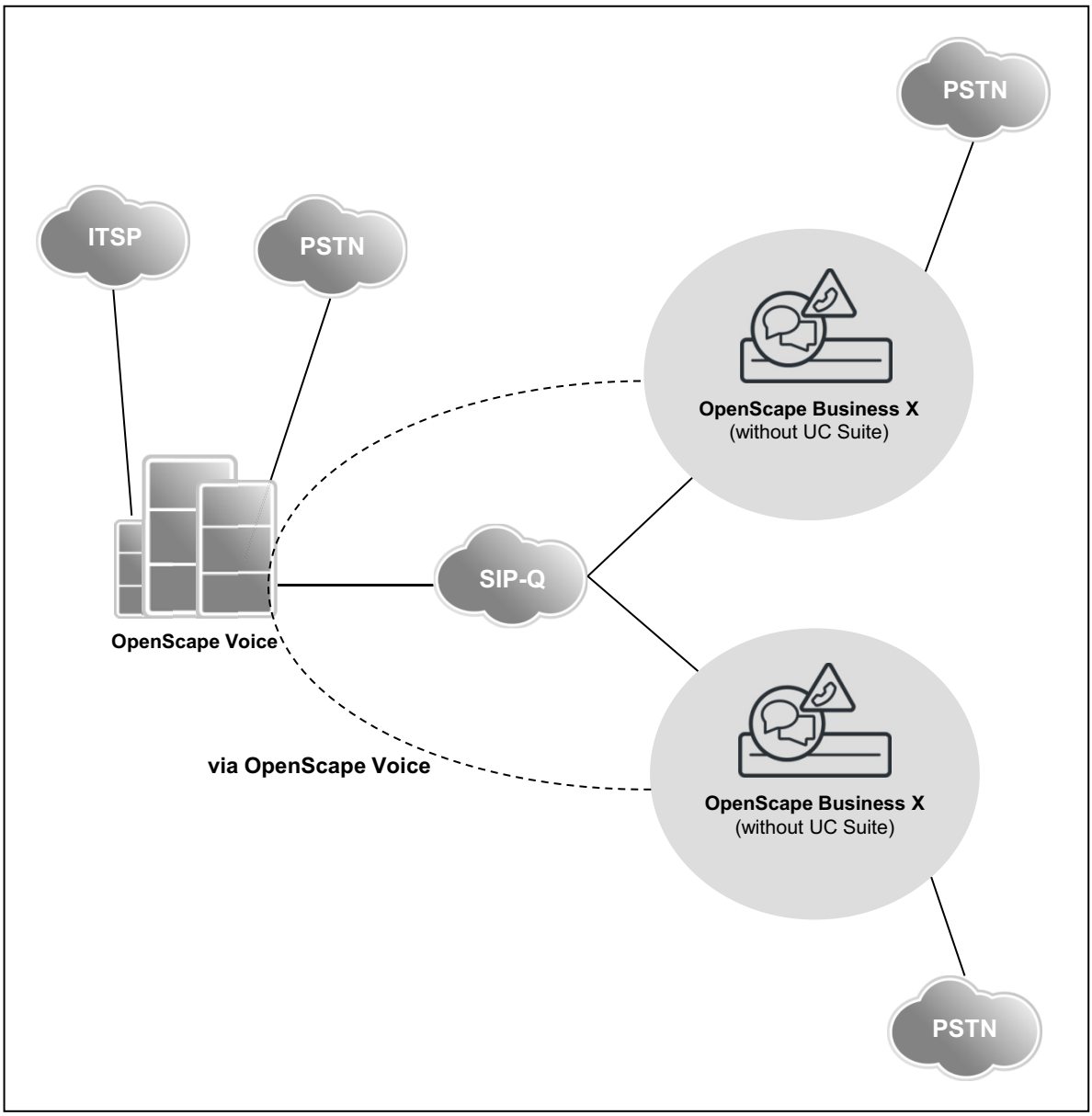
Mobility	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
Desksharing	Innerhalb eines Knotens; Netzweit, innerhalb der OpenScape Business Vernetzung mit DLS	Wird nicht unterstützt
Mobility mit DTMF-Steuerung des Systems	Lokal (wird bei OpenScape Business S nicht unterstützt)	Lokal
myPortal for Mobile (UC Suite)	Netzweiter Anwesenheitsstatus und Verzeichnisse (jeder Knoten benötigt dafür entweder UC Booster Server, UC Booster Card oder OpenScape Business S)	Wird nicht unterstützt
myPortal for Mobile (UC Smart)	Lokal, nicht für UC Booster Server, UC Booster Card und OpenScape Business S	Wird nicht unterstützt

Sonstige Funktionalitäten	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
Signalling and Payload Encryption SPE	Wird in OpenScape 4000/ HiPath 4000 - OpenScape Business Vernetzungen unterstützt. Wird nicht unterstützt bei UC-Verbindungen und Konferenzen	Wird in OpenScape 4000/ HiPath 4000 - OpenScape Business Vernetzungen unterstützt. Wird nicht unterstützt bei Konferenzen
DSS-Server	Netzweit innerhalb der OpenScape Business Vernetzung	Wird nicht unterstützt
Anrufübernahme	Wird nicht unterstützt	Wird nicht unterstützt

20.6.13 Szenario 5: Vernetzung von OpenScape Business X und OpenScape Voice

OpenScape Business X kann mit OpenScape Voice vernetzt werden.

INFO: Ein Einrichtebeispiel zur Vernetzung mit OpenScape Voice finden Sie im Unify Experts Wiki unter `http://wiki.unify.com/wiki/How_to_collection_and_tutorials_for_OpenScape_Business`



Netzwerkdaten

- OpenScape Business X stellt für OpenScape Voice eine netzweite Sprach- und Gateway-Funktionalität zur Verfügung
- Eine oder mehrere OpenScape Business X können als Gateway für digitale Ämter (ISDN, T1, CAS) verwendet werden
- An OpenScape Business X Gateways können folgenden Endgeräte betrieben werden: digital / analog / DECT / IP (HFA)
- UC wird seitens OpenScape Business X in dieser Vernetzung generell nicht unterstützt.
- Jedes Gespräch von einem Knoten auf einen anderen wird über OpenScape Voice geroutet.
- Die Konfiguration jedes Knotens erfolgt über den Expertenmodus.
- Der Rufnummernplan der OpenScape Voice basiert auf E.164, daher gibt es keine offene oder geschlossene Nummerierung.

20.6.14 Szenario 5: Netzweite Leistungsmerkmale

Maximalausbau	
Maximale Anzahl Knoten	abhängig von OpenScape Voice
Maximale Anzahl von Teilnehmern in einem einzelnen Kommunikationssystem	abhängig von OpenScape Business X
Maximale Anzahl von Teilnehmern im Netz	abhängig von OpenScape Voice

Administration	
WBM	Der Wizard Vernetzung kann nicht genutzt werden. Die OpenScape Voice wird über den Expertenmodus der OpenScape Business knotenweise administriert.
Manager E	Wird nicht empfohlen
UC-Administration	UC ist nicht relevant in Verbindung mit OpenScape Voice
Massendatenimport über csv-Dateien (Rufnummern, Durchwahlnummern, Namen)	Separat für jeden Knoten der OpenScape Business im Netzverbund

Lizenzierung	
Lizenzierung	Jeder Knoten einzeln, je OpenScape Business Knoten ist eine Netzlizenz erforderlich
Neue Lizenzierungsstruktur	Je OpenScape Business Knoten ist eine Netzlizenz erforderlich

Clients	
myPortal Smart	Nicht relevant, da UC in dieser Vernetzung nicht unterstützt wird
myPortal for Desktop	Nicht relevant, da UC in dieser Vernetzung nicht unterstützt wird
myPortal for Outlook	Nicht relevant, da UC in dieser Vernetzung nicht unterstützt wird
myAttendant	Nicht relevant, da UC in dieser Vernetzung nicht unterstützt wird
myAgent	Nicht relevant, da UC in dieser Vernetzung nicht unterstützt wird

OpenScape Business Attendant	
Support	Wird innerhalb des OpenScape Business Netzverbunds unterstützt. Ansonsten sind die internen Rufnummern (durch die Schnittstelle) auf 8 Zeichen beschränkt.
Instant Messaging	Lokal für jeden Knoten
VoiceMail	Lokal für jeden Knoten
Anwesenheitsstatus	Nicht möglich
Besetztanzeige	Lokal für jeden Knoten
Externes Verzeichnis	über LDAP
Zentraler Vermittlungsplatz	Wird nicht unterstützt

Company AutoAttendant	
Company AutoAttendant	Nicht relevant, da UC in dieser Vernetzung nicht unterstützt wird

Externe Applikationen	
OpenScape Business TAPI-Applikationen	Siehe *Application Connectivity*
Externe CSTA-Applikationen	
Application Launcher	
OpenScape Contact Center	Nicht relevant, da UC in dieser Vernetzung nicht unterstützt wird.

Telefonie	
SIP-Provider (ITSP)	Nicht unterstützt an OpenScape Business, Internet-Telefonate gehen ausschließlich über OpenScape Voice
PSTN-Provider	Lokal oder OpenScape Business als Gateway für OpenScape Voice
Survivability (Ausfallsicherheit im Falle eines Zusammenbruchs des Netzverbundes bzw. der OpenScape Business S)	Nicht unterstützt (da keine OpenScape Business S im Netz)
Wahl einer öffentlichen Rufnummer im eigenen Knoten	Wird unterstützt
Wahl einer öffentlichen Rufnummer in einem vernetzten Knoten	abhängig von der Konfiguration der OpenScape Voice

Mobility	
Desksharing	Lokal innerhalb eines Knotens von OpenScape Business
Mobility mit DTMF-Steuerung des Systems	Lokal
myPortal for Mobile	Nicht relevant, da UC in dieser Vernetzung nicht unterstützt wird.

Sonstige Funktionalitäten	
Signalling and Payload Encryption SPE	Wird unterstützt.

Einschränkungen und Hinweise zu den Leistungsmerkmalen

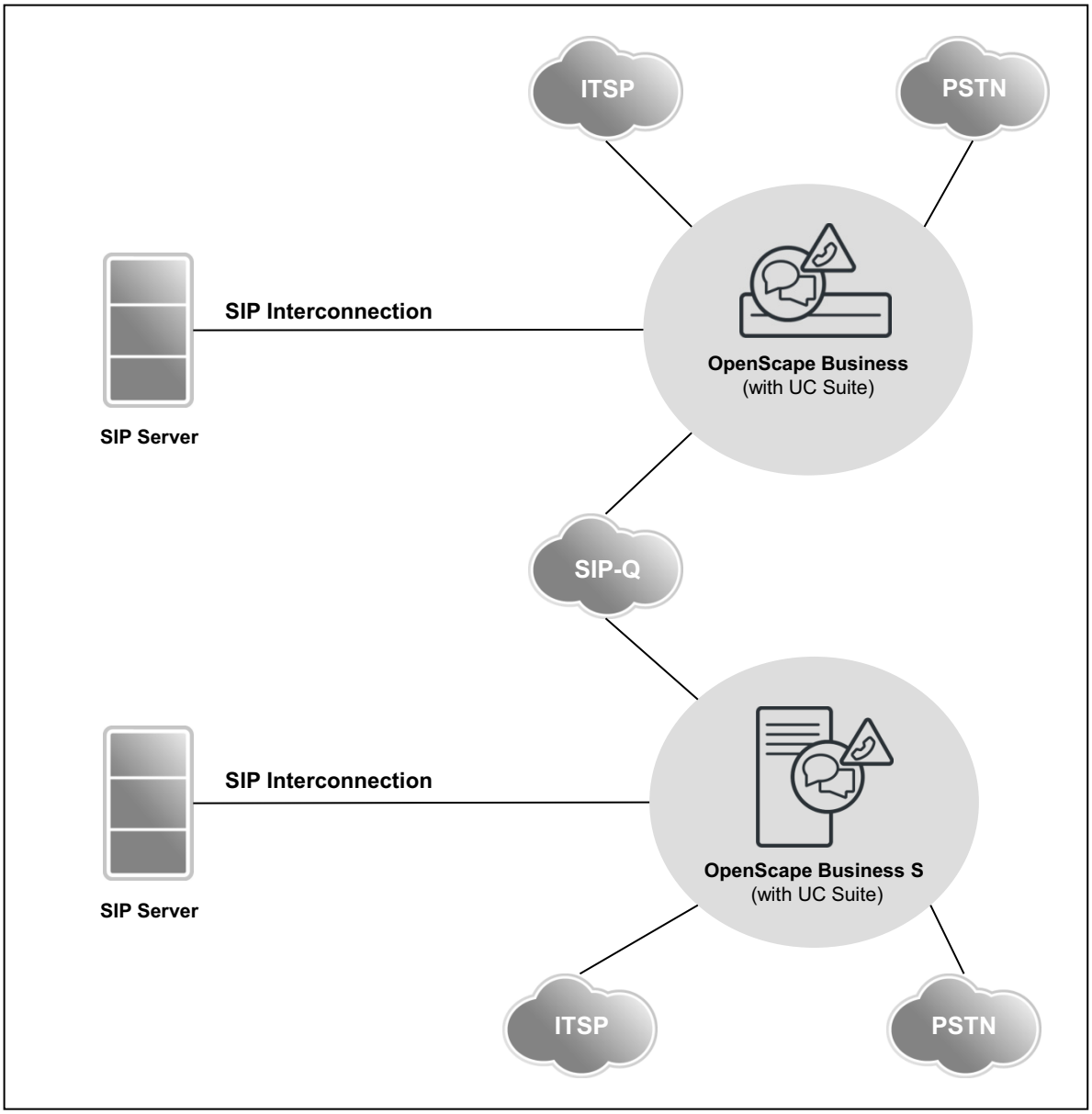
- Die Anschaltung von analogen Amtsleitungen an den OpenScape Business Gateways ist **nur** für Brasilien freigegeben (Aufgrund der Unterstützung von Line Reversal und Rückwärtsauslösen von analogen Amtsleitungen in Brasilianischen Ämtern).
- Eine Vernetzung von OpenScape Business-Gateways untereinander oder mit anderen Systemen als OpenScape Voice wird nicht unterstützt. Die Vernetzung der OpenScape Business-Gateways zur OpenScape Voice muss durch sternförmige Netzstruktur erfolgen.
- Path Replacement (Wegeoptimierung) über SIP-Q V2 wird nicht für die an einem OpenScape Business-Gateway angeschlossenen Endgeräte unterstützt.
- Um schlechte Sprachqualität bei Transit-Leitungsverbindungen zu vermeiden, sollte der Sprach-Codec G.711 verwendet werden. Der Codec G.729 wird nicht empfohlen, da durch Leistungsmerkmale wie Konferenz und Anrufumleitung Transit-Leitungsverbindungen entstehen können, da Path Replacement (Wegeoptimierung) nicht unterstützt wird.
- Keine systemübergreifende Unterstützung von Leistungsmerkmalen, wie zum Beispiel Anrufübernahmegruppen, Gruppenrufe und Sammelanschlüsse zwischen OpenScape Voice und OpenScape Business Gateways. Die Gruppen dürfen entweder nur OpenScape Voice oder nur OpenScape Business Teilnehmer beinhalten.
- Verschlüsselung (SPE) zwischen OpenScape Voice und OpenScape Business Gateways wird unterstützt. Die Verbindung zwischen OpenScape Voice und OpenScape Business muss mittels des Verschlüsselungsproto-

kolls TLS erfolgen. SRTP (SDES) wird bei einer Vernetzung mit der OpenScape Voice V7R1 nicht unterstützt.

- Unterstützt wird ausschließlich die Vernetzung mit E.164-Rufnummernplan.
- Für die an OpenScape Business Gateways angeschlossenen IP Endgeräte (HFA) gilt: für jede aktive OpenScape Business/OpenScape Voice-Verbindung werden 2 B-Kanäle pro HFA-Endgerät benötigt (1 B-Kanal pro TDM-Endgerät). Die Notwendigkeit dieser zusätzlichen DSP-Ressourcen sollte überprüft und berücksichtigt werden.

20.6.15 Szenario 6: Anbindung von externen Anschaltungen an OpenScape Business über SIP-Interconnection

An OpenScape Business können externe Anschaltungen über SIP-Interconnection angebunden werden, um z. B. Applikation wie OpenScape Alarm Server, OpenScape 4000/HiPath 4000, OpenScape Voice oder andere zertifizierte SIP-Server nutzen zu können.



Voraussetzungen

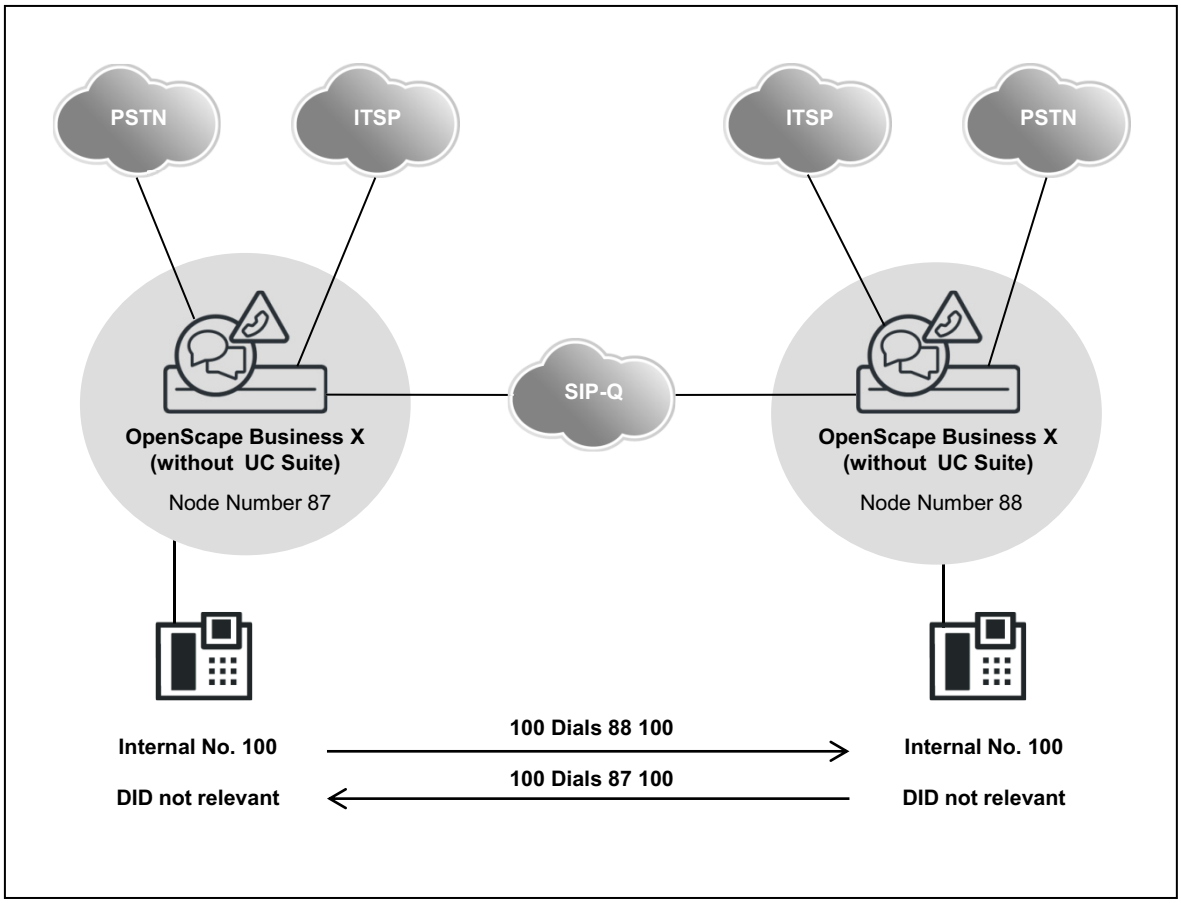
- Es dürfen nur zertifizierte Applikationen angeschlossen werden wie z. B. OScAR-Eco.
- Ein externer SIP-Server kann über SIP- oder SIP-Q-Protokoll angeschlossen sein.
- Es stehen maximal zwei Richtungen für SIP-Interconnection zur Verfügung. Eine davon wird für UC-Suite benötigt, falls vorhanden.

Weiterführende Information finden Sie im

- Experten-Wiki für Telefone, Kommunikationssysteme und UC: `http://wiki.unify.com`

20.6.16 Szenario 7: Offene Nummerierung in OpenScape Business X Netzwerken

Ein Netzverbund mit offener Nummerierung kann eingerichtet werden, wenn zwei (oder mehrere) Kommunikationssystem vernetzt werden, bei denen die Nummerierung sich überschneidet (nicht eindeutig ist im Netzverbund).



Netzwerkdaten

- Netzweite Sprachvernetzung über OpenScape Business
- UC-Leistungsmerkmale werden nicht unterstützt. Smart VoiceMail und Company AutoAttendant (UC Smart) können lokal genutzt werden.
- Jeder Anruf innerhalb eines Knotens erfolgt mit interner Rufnummer
- Jeder Anruf zu einem anderen Knoten erfolgt mit Knotennummer (plus interner Rufnummer)
- Konfiguration jedes Knotens über den Expertenmodus. Der Wizard Vernetzung ist gesperrt, sobald eine Knotennummer für offene Nummerierung konfiguriert ist.
- Amtszugang (PSTN) und ITSP sind lokal an jedem Knoten

- keine OpenScape Business S erlaubt, da die integrierte UC-Suite des Softswitches nicht mit offener Nummerierung zusammenarbeitet

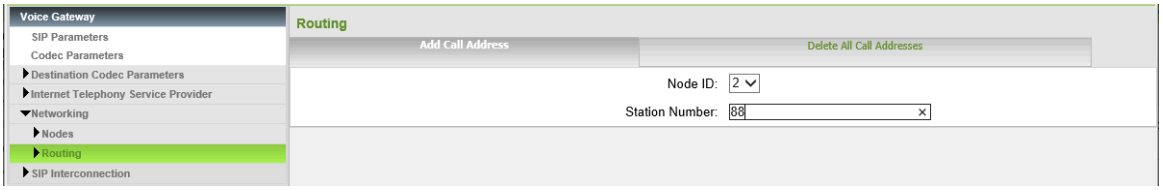
20.6.17 Szenario 7: Konfiguration

Offene Nummerierung einrichten

1. Offene Nummerierung für das Kommunikationssystem freigeben über das Systemflag **Offene Nummerierung**
2. Eigene Knotennummer eintragen (im Beispiel "87")

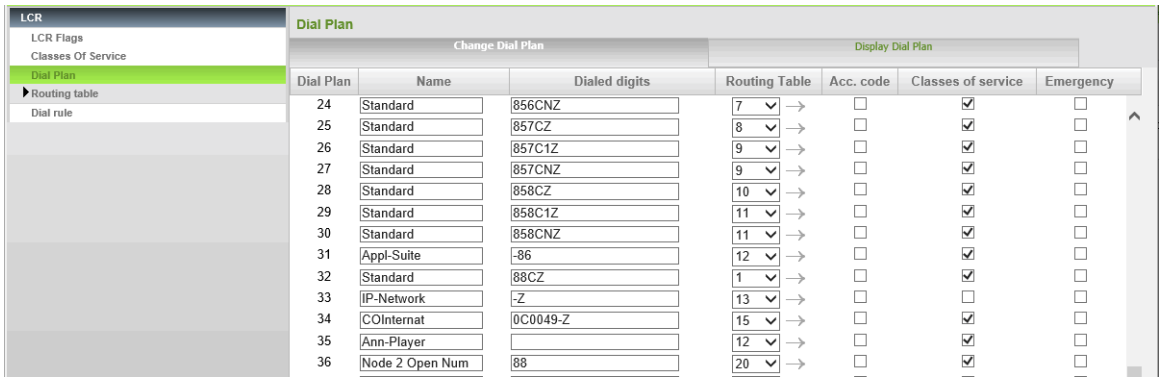
Knoten (Routing) einrichten

1. Die Zielknoten werden über
   Sprachgateway > Networking > Knoten > Routing addressiert (im Beispiel "88").
2. Bei einer offenen Nummerierung kann der Wizard Vernetzung nicht genutzt werden, dies wird durch das Systemflag **Offene Nummerierung** verhindert.

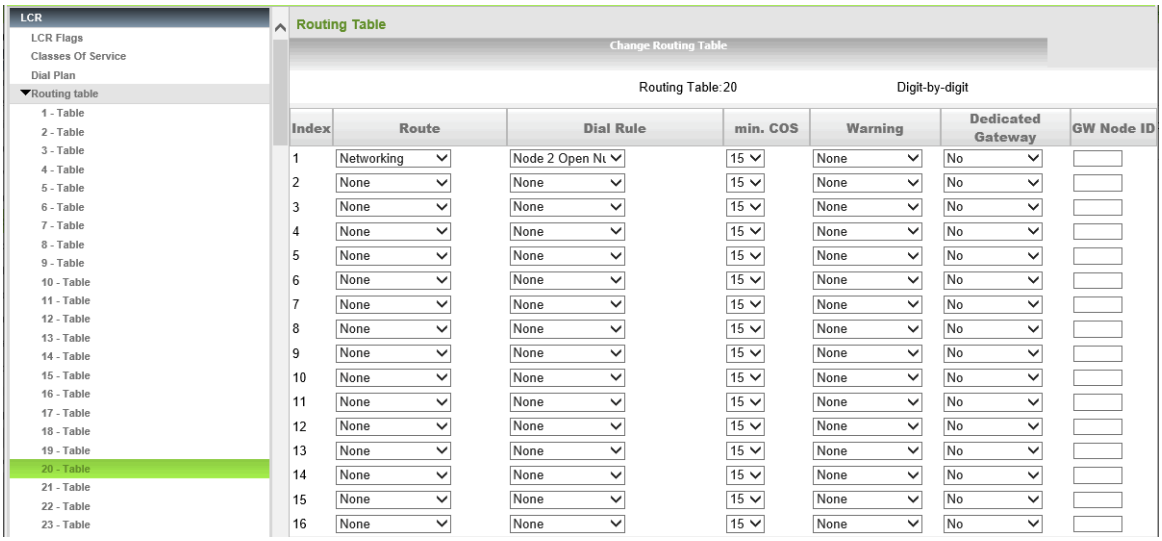


LCR einrichten

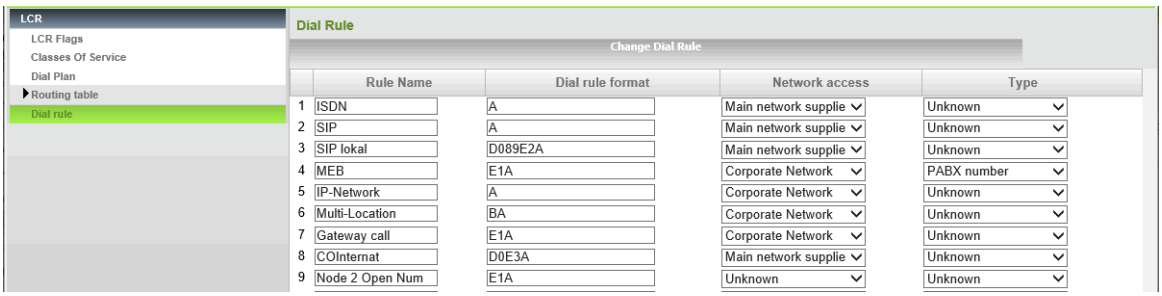
1. Die Wahlregel "Node 2 open Num" für die Knotennummer definieren und die zugehörige Routing Tabelle auswählen.



2. Anzeige der konfigurierten Route



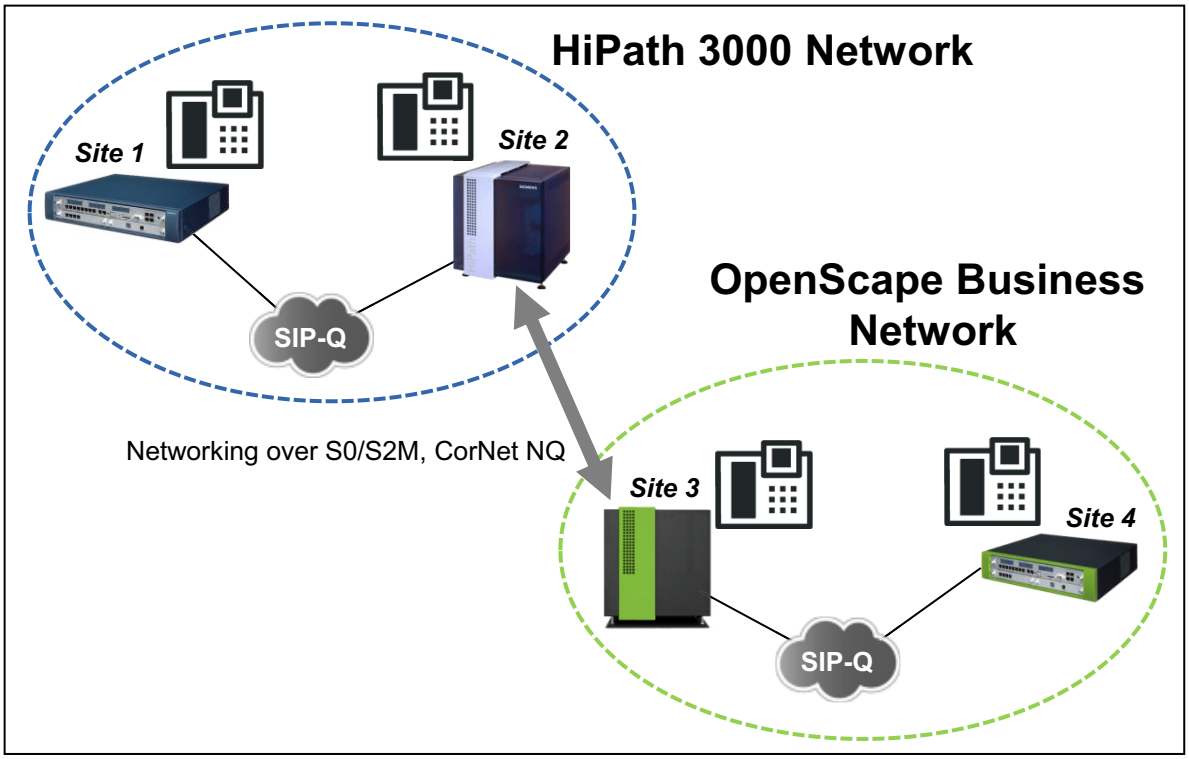
3. Den Namen der Route "Networking" und die dazugehörige Wahlregel "Node 2 open Num" eingeben.



20.6.18 Szenario 8: Vernetzung über ISDN

OpenScape Business Systeme können sowohl untereinander als auch mit den Kommunikationssystemen HiPath 3000 und OpenScape 4000/HiPath 4000 über digitale Verbindungsleitungen vernetzt werden. Die Anschaltung kann sowohl über S0- als auch über S_{2M}-Leitungen erfolgen.

Vernetzung mit HiPath 3000



Das vorhandene HiPath 3000 Netz bleibt (zunächst) unangetastet. Die Erweiterung des Netzes erfolgt mit OpenScape Business. HiPath 3000-Knoten können bei Bedarf schrittweise in das OpenScape Business Netz migriert werden.

Jeder übergreifende Anruf HiPath 3000/OpenScape Business wird über entspr. TDM-Gateways geführt (S0- oder S2M mit CorNet NQ-Protokoll, ggf. QSIG als Hersteller-unabhängiges Protokoll).

Es gelten die folgenden Randbedingungen:

- Separate Lizenzierung HiPath 3000/OpenScape Business
- Separate Administration HiPath 3000/OpenScape Business
- Empfehlung: Geschlossene Nummerierung im Gesamtnetz. Bei offener Nummerierung kann es ggf. zu Fehlverhalten bzgl. CLIP und bei Journaleinträgen/Anruferlisten kommen.
- Empfehlung: Ausschließlich Codec G.711 verwenden, um gute Sprachqualität im Gesamtnetz zu gewährleisten.
- Die Anzahl der B-Kanäle ist entsprechend des zu erwartenden Gesprächsaufkommens zu berücksichtigen.
- OpenScape Business benötigt in jedem Fall eine Networking Lizenz.

Anschaltung von Fremdsystemen über QSIG

Eine Vernetzung zu Kommunikationssystemen anderer Hersteller ist mit dem herstellerübergreifenden Protokoll QSIG möglich.

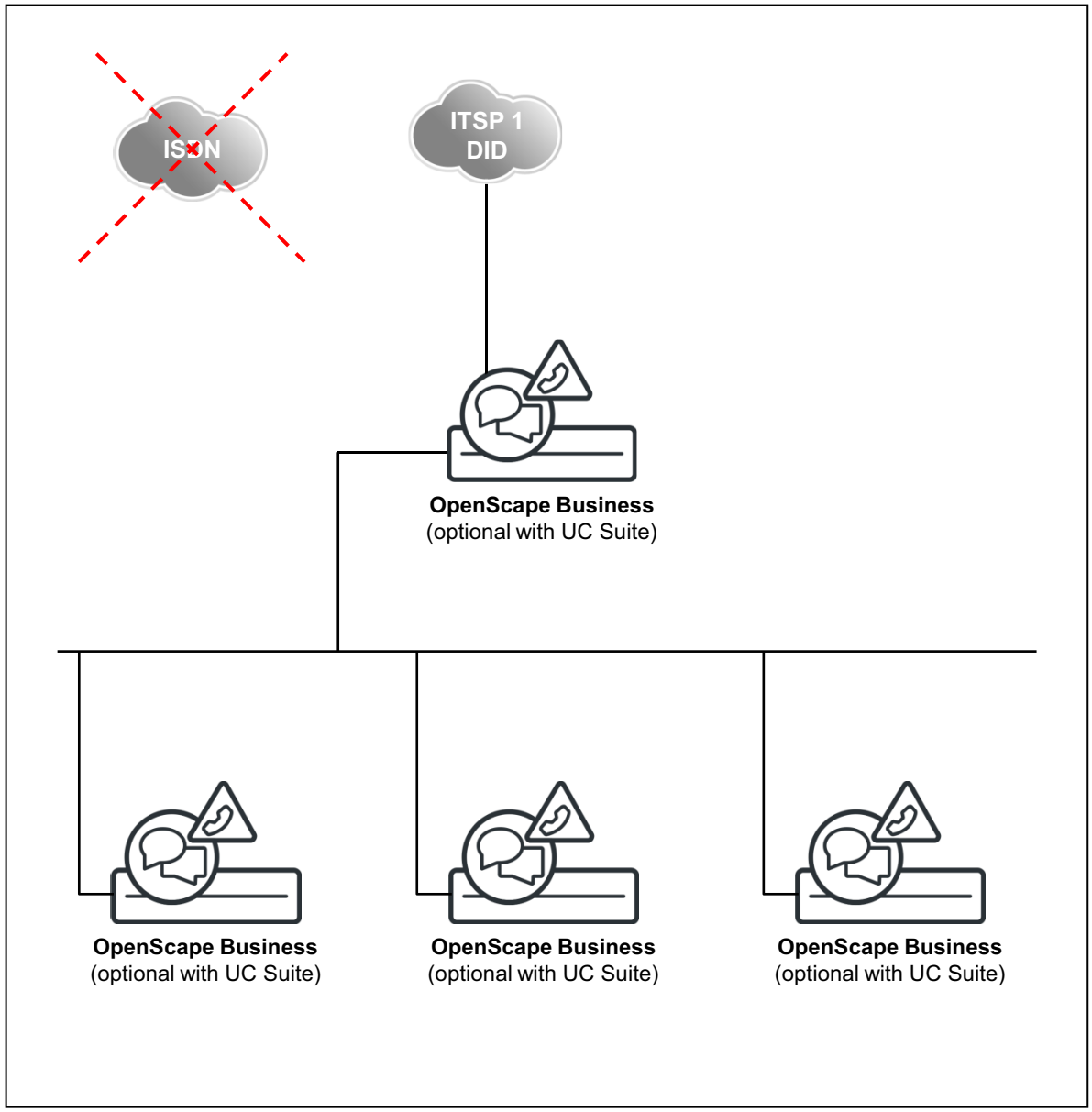
Bei Anschaltung von Fremdsystemen mit dem QSIG-Protokoll ist folgendes zu beachten:

- Prüfung der QSIG-Varianten der betroffenen Fremdsysteme auf Kompatibilität (QSIG V1 auch QSIG nach ECMA-Standard genannt, bzw. QSIG V2 auch QSIG nach ISO-Standard genannt)
- Gegenüberstellung der Featuresets der betroffenen Systeme. Daran kann abgelesen werden, inwieweit der theoretisch zu erwartende Leistungsumfang, d.h. der deckungsgleiche Anteil beider Featuresets den Kundenwünschen entspricht.
- Zur weiteren Absicherung der zu erwartenden Funktionalität wird ein Anschaltetest vor Ort empfohlen. Dabei ist insbesondere das Interworking mit anderen Vernetzungsprotokollen bzw. Amtsprotokollen zu beachten.

20.6.19 Szenario 9: OpenScape Business Netzverbund mit zentralem ITSP-Amtsanschluss

Ein reiner OpenScape Business Netzverbund kann statt ISDN mit einem zentralen, durchwahlfähigen ITSP-Amtsanschluss realisiert werden.

Vernetzung mit zentralem, durchwahlfähigem ITSP-Amtsanschluss



Folgendes ist bei der Planung von Kundennetzen zu beachten:

- **Ein** zentraler, durchwahlfähiger ITSP-Amtsanschluss für das komplette OpenScape Business Netz.
- Registrierung an genau einem Ortsnetz, d.h. alle Knoten des Netzes nutzen genau eine Amtsrufnummer, z.B. 0049 89 7007-xxxxx.
- Die vernetzten Knoten können für Notfälle, d. h. bei Ausfall des zentralen ITSP-Zugangs, eigene Amtsanschlüsse für ausgehende Verbindungen verwenden. Unter Umständen ist in diesem Fall eine korrekte Anrufer-Identifizierung nach außen nicht möglich. Notrufe können ggf. nicht korrekt zugestellt werden. Die kommende Erreichbarkeit über diesen lokalen

Anschluss ist ebenfalls mit Restriktionen verbunden. Aus genannten Gründen werden lokale Anschlüsse nicht empfohlen, werden aber technisch nicht verhindert.

- Aus dem gleichen Grund werden am zentralen Knoten keine zusätzlichen ISDN-Anschlüsse empfohlen, technisch aber nicht verhindert.
- Es gelten alle Regeln für Wahlbewertung und Call-Routing für OpenScape Business-Einzelsysteme und -Netze. Die Rufnummernzuordnung der ITSP-Amtsrufnummern erfolgt in diesem Fall ausschließlich über die Durchwahl-Konfiguration des Teilnehmers (nicht über die Mapping-Tabelle, siehe ITSP-Konfiguration Kapitel 9.2).

20.7 Zentraler Abwurfplatz im Netzverbund (nicht für USA)

OpenScape Business ermöglicht, ankommende Rufe, die keinem Teilnehmer zuzuordnen sind oder nicht beantwortet werden, an einen festzulegenden Abwurfplatz im Netzverbund umzuleiten, damit kein Anruf verloren geht.

Wenn der zentrale Abwurfplatz im Netzverbund über ISDN konfiguriert ist, so ist die Funktionsweise identisch mit der Funktionsweise ohne Vernetzung.

In Verbindung mit einem ITSP-Amt ergeben sich für den zentralen Abwurfplatz einige Einschränkungen, da jeder Knoten grundsätzlich seinen eigenen ITSP hat:

- Die ITSP-Abwurfkriterien gelten nur für den jeweiligen Knoten.
- Es funktionieren Abwurf im Freifall, bei Besetzt, bei unvollständiger Wahl, bei Falschwahl und bei unbeantwortetem Wiederanruf.
- Die Abwurfarten "Falschwahl" und "Unvollständig" funktionieren beim ITSP nicht.
- Unvollständige oder falsche Rufnummern werden mit Besetztsignal an den ITSP zurückgegeben.

Wenn ein zentraler Abwurfplatz in einem Netzverbund genutzt werden soll, müssen in jedem Knoten virtuelle Teilnehmer konfiguriert werden. Diese virtuellen Teilnehmer werden über den Netzverbund fest zum myAttendant Benutzer umgeleitet.

Beispiel für ITSP-Amt: ITSP-Anlagenrufnummer ist 0211-23456789 + ITSP-Durchwahlnummer, öffentlich wird die Rufnummer 0211-23456789-0 als zentrale Nummer des Kommunikationssystems bekannt gegeben.

- Teilnehmer 100 ist myAttendant mit eigener ITSP-Durchwahlnummer 100 und einem virtuellem Teilnehmer 199 mit ITSP-Durchwahlnummer "0".
- In der ITSP-Mapping-Liste jedes Knotens wird die ITSP-Durchwahlnummer "0" dem eigenen virtuellen Teilnehmer zugeordnet.
- Unter **Kommende Rufe/Rufweiterschaltung** werden die virtuellen Teilnehmer auf Teilnehmer 100 verwiesen.
  Erstes Ziel: eigener virtueller Teilnehmer
  Zweites Ziel: Teilnehmer 100 im Zielknoten
  Rufzeit 5 Sekunden

Zur besseren Identifikation der Anrufe ist es empfehlenswert, die virtuellen Teilnehmer aller Knoten über die Applikation myAttentand (unter **Einrichtung**/

myAttendant/**DuWas**) mit ihrer Rufnummer (DID) und einem Namen (z. B. Firma) zu versehen. Damit ist im Fenster **Aktive Anrufe** von myAttendant eine ausführlichere Identifikation des Anrufers möglich.

20.7.1 Wie Sie den zentralen Abwurfplatz im Multi-Gateway-Netzverbund konfigurieren

Einrichtebeispiel für einen zentralen Abwurfplatz im Multi-Gateway-Netzverbund über die vorgeschalteten OpenScape Business Gateways. Alle Anrufe, die in einem Knoten eingehen und die Abwurfkriterien erfüllen, müssen zu OpenScape Business S werden, wo sich der zentrale AutoAttendant befindet.

Voraussetzungen

- OpenScape Business S ist Master (alle HFA- und SIP-Teilnehmer sind hier angemeldet).
- Mehrere OpenScape Business X sind als Slave-Knoten (mit ISDN, HKZ, ITSP, etc. als Amtszugang) eingerichtet. Die Knoten können sich am gleichen Ort oder an unterschiedlichen Standorten befinden (unterschiedliche Vorwahlen).

Schritt für Schritt

1) Einrichten eines virtuellen Teilnehmers an OpenScape Business.

a) Einrichten eines virtuellen Teilnehmers mit Namen "Abwurf 22 System2"

2) Einrichten eines Zentralen Abwurfplatzes mit Abwurfkriterien an OpenScape Business.

a) **Experten-Modus**

b) **Grundeinrichtung** > **System** > **Abwurf/VPL/Hotline**

c) Virtuellen Teilnehmer 22 unter **Abwurfplatz** bei **Tag und Nacht** auswählen.

d) Folgende Parameter für den Teilnehmer 22 unter **Abwurfplatz** bei **Abwurf** eingeben:

Name	Abwurf 22 System2
Durchwahl	xxxxxxx22
Endgeräte Typ	virtuell

e) Aktivieren der eingegebenen Parameter unter **Abwurfplatz** bei **Abwurf** .

f) Einrichten des virtuellen Teilnehmers unter **Abwurfplatz** bei **Codeschloss**.

3) Einrichten der Rufweiterschaltung an OpenScape Business.

a) Einrichten der Rufweiterschaltung des virtuellen Teilnehmers 22 über den Netzverbund zu OpenScape Business S.

b) **Experten-Modus**

c) **Kommende Rufe** > **Rufweiterschaltung**

d) Virtuellen Teilnehmer 22 auswählen

e) Weiter zu **Rufweiterschaltung für Teilnehmer parametrieren**

f) dann an: **externes Ziel** (AutoAttendant Warteschlangen-Rufnummern eingeben z. B. 7410)

g) **Richtung =** Netzwerk auswählen (Die AutoAttendant Warteschlangen-Rufnummer 7410 muss gezielt im LCR geroutet werden, unter Umgehung der -Z Default Regel 33).

INFO: Alternativ kann der Abwurfplatz der OpenScape Business S verwendet werden. damit ist die Konfiguration unabhängig ob myAttendant oder der OpenScape Business Attendant zum Einsatz kommt.

---

4) Konfigurieren des Routings für OpenScape Business.

Die AutoAttendant Warteschlangen-Rufnummer 7410 muss gezielt im LCR geroutet werden (unter Umgehung der -Z Default Regel 33).

unter **Wahlplan**:	**Name** einrichten (VSL Queue Pilot)
	Rufnummer unter **Gewählte Ziffern** eingeben (7410)
	Wegetabelle auswählen (XX)
unter **Wegetabelle** XX:	**Richtung** = Netzwerk auswählen
	Wahlregel zuordnen
	Unter **Dediziertes Gateway** den Eintrag **Erzwungen** auswählen
	GW Knoten ID der OpenScape Business S eintragen
unter **Wahlregel**:	**Regelname** eintragen
	Wahlregelformat D7410 (Queue Pilot Nummer) eintragen
	Verfahren des Netzanbieters: Corporate Network auswählen
	Type: Unbekannt auswählen

5) Einrichten einer Warteschlange an OpenScape Business S.

a) Einrichten einer Warteschlange (Queue Pilot) mit einer CCV, z. B. **Nebenstellenwahl**, **Nach Name wählen**, **Aktion nach Ziffern**.

6) Einrichtung einer Rufweiterschaltung an OpenScape Business S.

a) Einrichten der Rufweiterschaltung der Queue Pilot 7410 in OpenScape Business S.

b) **Experten-Modus**

c) **Kommende Rufe** > **Rufweiterschaltung**

d) Queue Pilot 7410 auswählen

e) Weiter zu **Rufweiterschaltung für Teilnehmer parametrieren**

f) zuerst an: **externes Ziel** (AutoAttendant Warteschlangen-Rufnummern eingeben z. B. 7410)

g) dann an: **Sprachbox** auswählen

20.8 Presence Manager

Der Presence Manager ermöglicht die netzweite Signalisierung der vermittlungstechnischen Teilnehmerzustände “Frei", “Besetzt" und “Ruf" an den LEDs der HFA-Telefone. Voraussetzung dafür ist eine geschlossene Nummerierung und mindestens ein UC Booster Server im Netzverbund. Pro Knoten ist eine Netzwerklizenz erforderlich.

Bei Frei-Zustand ist die entsprechende LED aus, im Belegt-Zustand ist sie dauernd an, im Rufzustand blinkt die LED. Im Rufzustand kann dieser Ruf durch Betätigen der entsprechenden Taste übernommen werden.

Die Signalisierung der vermittlungstechnischen Zustände eines Teilnehmers ist nur möglich, wenn der Presence Manager auf diesen Teilnehmer einen CSTA-Monitorpunkt setzen kann. Zur Generierung von CSTA-Meldungen muss ein Masterknoten gestartet sein.

Die Konfiguration der Tasten erfolgt durch den Anwender. Bei der Programmierung am Telefon selbst besteht kein Unterschied, ob es sich um eine interne oder netzweite Rufnummer handelt.

Der Presence Manager ist ein Dienst ohne Benutzeroberfläche. Es sind keine Einstellungen vorzunehmen, da alle Daten automatisch durch einen Datenabgleich abgeleitet werden.

Gruppen werden nicht durch Presence Manager unterstützt. Es erfolgt keine LED-Signalisierung und es besteht keine Möglichkeit der Anrufübernahme. MULAPs werden dagegen vom Presence Manager unterstützt.

Presence Manager unterstützt aktiv keine SIP- und S_0-Telefone.

20.9 Synchronisationsstatus im Netzverbund

Bei einem Netzverbund wird der Synchronisationsstatus im Admin-Portal und der Registrationsstatus der einzelnen Knoten durch farbige Buttons angezeigt. Die Anzeige des Synchronisationsstatus gilt für Netzknoten des Kommunikationssystems, nicht für OpenScape 4000/HiPath 4000 und OpenScape Voice Knoten.

Anzeige des Synchronisationsstatus

Anzeige	Farbe	Bedeutung für den Master	Bedeutung für den Slave
Synchronisations Status (Anzeige auf der Startseite des Admin-Portals)	Rot	-	Die IP-Adresse des Master-Knotens ist konfiguriert aber das Slave-System konnte sich nicht registrieren. In zyklischen Abständen versucht sich der Slave beim Master zu registrieren.
	Gelb	-	Slave ist beim Master registriert, aber die Rufnummern sind nicht konsistent im Netzverbund. Dies kann nach einem Backup/Restore oder nach der ersten Registrierung der Fall sein.
	Grün	Wenn ein Knoten als Master konfiguriert ist, dann erscheint der Status Grün.	
Registrationsstatus der einzelnen Knoten (Anzeige im Dialog Netzwerk>Knotensicht)	Rot	Slave ist konfiguriert; das System hat sich aber noch nie registriert.	Slave ist konfiguriert; das System hat sich aber noch nie registriert.
	Grün	Das System ist bereits registriert. HiPath 3000 Systeme sind immer grün, da sie keine Registrierung benötigen.	Das System ist bereits registriert. HiPath 3000 Systeme sind immer grün, da sie keine Registrierung benötigen
Alive (Anzeige im Dialog Netzwerk>Knotensicht)	Rot	Knotenspezifischer Blick auf den Netzverbund: Alle Knoten, die rot markiert sind, können nicht erreicht werden. Die Gründe dafür können Netzwerkprobleme oder ein Ausfall des Kommunikationssystems sein. Diese Anzeige zeigt auch den Status der HiPath 3000 Knoten an.	
	Grün	Der (fremde) Knoten ist über das Netzwerk erreichbar. Der eigene Knoten wird stets grün dargestellt.	

20.9.1 Manuelle Synchronisierung im Netzverbund

Wenn nach der Konfiguration von Rufnummern / Namen (Interne- oder Durchwahlrufnummern) diese nicht automatisch in den anderen Systemen eines Netzverbundes synchronisiert werden, kann eine manuelle Synchronisierung angestoßen werden. Die manuelle Synchronisierung im Netzverbund funktioniert nur in homogenen Vernetzungen.

Der Synchronisierungs-Vorgang überträgt ausschließlich Konfigurationsänderungen.

Steht die Statusanzeige im Admin-Portal auf "Rot", kann durch Aktivieren der Synchronisierungs-Schaltfläche versucht werden, die Synchronisierung der Daten an den Master manuell zu starten.

Für den Fall, dass bereits konfigurierte Systeme im Netzwerk untereinander nicht mehr telefonieren können, muss die Ursache für diese Störung anderweitig gesucht werden. Ist der Alive-Status einzelner Knoten "Rot", ist dies ein Hinweis auf Netzwerkprobleme oder es gibt andere Gründe, warum der Knoten im

Netzwerk nicht erreichbar ist. In diesen Fällen bringt eine Aktivierung der Synchronisierungs-Schaltfläche keine Abhilfe.

Master

Bei Aktivierung auf dem Master-Knoten werden die Slave-Knoten aufgefordert, Rufnummern und Namen des Systems vom Master zu aktualisieren.

Slave

Bei Aktivierung auf einem Slave-Knoten werden die Rufnummern und Namen des Systems an den Master aktualisiert. Gleichzeitig findet ein erneutes Registrieren des Slave-Knotens beim Master-Knoten statt.

20.9.2 Wie Sie eine Synchronisierung manuell starten

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Restart / Reload**.

3) Aktivieren Sie die Schaltfläche **Sync Network** um die manuelle Synchronisierung zu starten.

20.10 Survivability

Survivability ist ein Leistungsmerkmal innerhalb einer Vernetzung von OpenScape Business S mit OpenScape Business X Gateways. Ist die OpenScape Business S ausgefallen oder aufgrund von Netzwerkfehlern nicht erreichbar, können sich die an der OpenScape Business S angemeldeten Systemtelefone (HFA) an einem OpenScape Business X Gateway (Standby-Gateway) anmelden. Die Rufnummern der Systemtelefone bleiben nach der Ummeldung erhalten. Damit ist weiterhin die Basis-Telefonie gewährleistet, die Leistungsmerkmale der Applikationen wie z. B. myPortal, Voicemail und CTI werden vorübergehend ausgesetzt.

Nachdem die OpenScape Business S wieder sicher erreichbar ist, wechseln die Systemtelefone automatisch zurück zur OpenScape Business S.

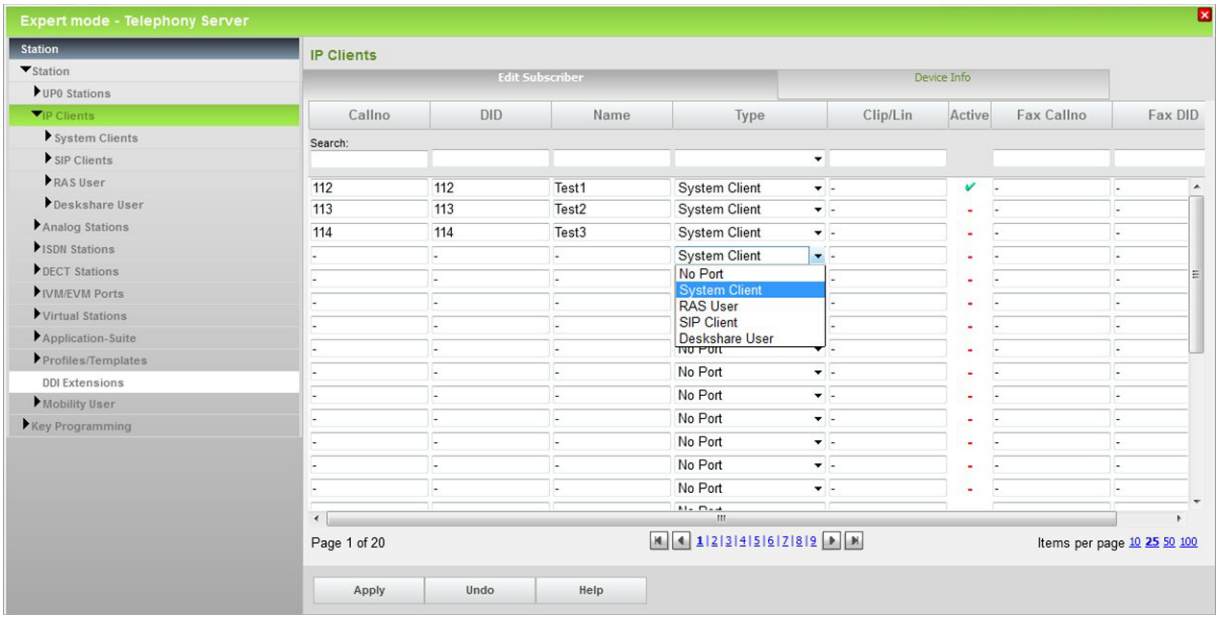
Die Zeit für das Umschalten auf das Standby-Gateway kann bis zu 30 Minuten dauern.

Wenn die OpenScape Business S ausfällt, wird für eine fest eingestellte Zeit (10 Minuten; nicht veränderbar) versucht, diese wieder zu erreichen. Erst wenn diese Zeit abgelaufen ist, melden sich die dafür vorgesehenen Systemtelefone an dem Standby-Gateway an. Der aktuellen Status der angemeldeten Telefone ist im **Expertenmodus > Diagnosedaten** einsehbar.

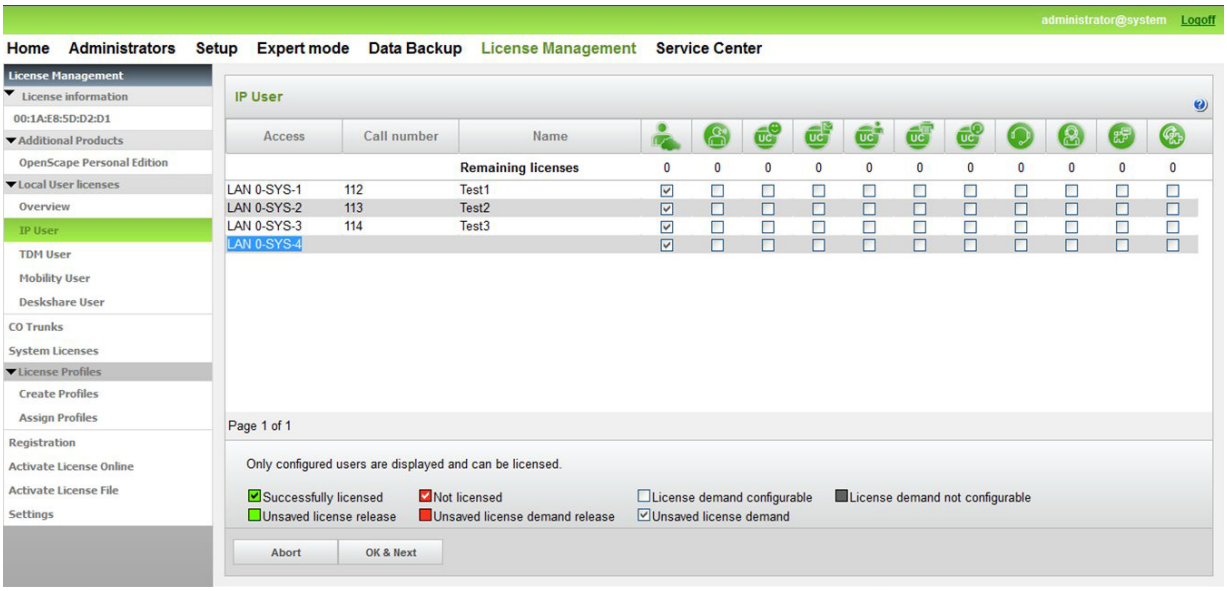
Die Survivability-Einstellungen werden an den Systemtelefonen konfiguriert. Wenn die OpenScape Business S ausfällt, versuchen die Telefone erst mehrmals diese wieder zu erreichen. Ein Time Out bzw. wie oft sich die Telefone wieder versuchen anzumelden kann über das Administrationsmenü der Telefone über "System Redundancy" konfiguriert werden. Die Defaulteinstellung für das Time Out ist 30 Sekunden mit 1 Wiederholungsversuch. Danach registrieren sich die Telefone am Standby-Gateway. Die automatische Rückanmeldung an der OpenScape Business S ist ebenso auf den Systemtelefonen zu konfigurieren.

Voraussetzung für Survivability ist:

- Für die Anzahl der an OpenScape Business S angeschlossenen Systemtelefone, die im Falle eines Netzknotenausfalls "gerettet" werden sollen, müssen am Standby-Gateway freie IP-Ports vorhanden sein.
- Für diese freien Ports am Standby-Gateway müssen Teilnehmer ohne Namen und Rufnummer eingerichtet sein.



- Die Teilnehmer müssen als Systemtelefone (System Client) konfiguriert und eine IP-User-Lizenz haben. Der Teilnehmer kann im Falle von Survivability ausschließlich Telefonie nutzen.



20.10.1 Wie Sie Survivability konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Navigieren Sie im Menübaum zu **Teilnehmer > IP Clients**. Bei einem OpenScape Business Master-System erscheint das Fenster **Secondary Gateway**.

3) Wählen Sie unter **Node ID** die OpenScape Business aus, die im Notfall die Teilnehmer der OpenScape Business S übernehmen soll.

4) Aktivieren Sie das Kontrollkästchen **Emergency** für die Notfallteilnehmer.

5) Die Einträge für **Emergency Call no** und **Call no DID** sind vorgeleistet und können ggf. angepasst werden.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

20.11 Entfernung eines Knotens aus dem Netzverbund

Wenn ein Knoten aus dem Netzverbund entfernt werden soll, ist es wichtig das der Knoten nicht mehr erreichbar ist. Sonst versucht dieser Knoten sich selbständig wieder im Netzverbund anzumelden.

Vorgehensweise

Das Löschen eines Knotens erfolgt über den Wizard Vernetzung, wobei immer alle beteiligten Knoten entfernt werden müssen.

Wird nur einer der beteiligten Knoten gelöscht, werden weiterhin Daten von einer OpenScape Business zur anderen übertragen und es kann zu Inkonsistenzen im internen Verzeichnis kommen, d. h. die Benutzer erscheinen nicht im Benutzerverzeichnis und können somit z. B. myPortal for Desktop nicht nutzen.

- Alle Strecken (Routing) zu den zu entfernenden Knoten unterbrechen.
- Administration des Netzverbundes
- Im Wizard Vernetzung alle Knoten entfernen
  Für die betroffenen Slave-Knoten "Kein Netzwerk" eintragen und den Master-Knoten aus der Registrations-Liste enternen.

21 Anschaltungen

Anschaltungen sind externe Geräte (wie z. B. ein Ansagegerät oder eine Türsprechstelle mit Türöffner), die an die Schnittstellen des Kommunikationssystems angeschlossen werden. Über eine IP-fähige Kamera kann die Videoüberwachungslösung Gate View genutzt werden.

21.1 Analoges Ansagegerät

Ein analoges Ansagegerät kann an eine a/b-Schnittstelle angeschlossen werden, um darüber eigene Ansagen abspielen zu können (z. B. für den zentralen AutoAttendant oder als Ersatz für die Wartemusik).

> ***INFO:*** Bitte vergewissern Sie sich vorher, dass Sie mit der Benutzung von Ansagen oder Wartemusik keine Copyright-Verletzungen begehen.

Pro Kommunikationssystem können bis zu 16 Ansage-Quellen konfiguriert werden, wie z. B. Mediaserver, Announcement Player oder auch analoge Ansagegeräte.

Dabei können die folgenden Typen von Ansagegeräten verwendet werden:

- Ansagegeräte, welche bei Aktivierung stets beim Textanfang starten (z. B. Begrüßungsansage)
- Ansagegeräte, welche über eine Endlos-Wiedergabe verfügen (z. B. für Wartemusik)

Das Ansagegerät muss sich wie ein Teilnehmer verhalten, d. h. sich melden, die Ansage einspielen und das Gespräch vermitteln (in Rückfrage gehen, wählen und auflegen).

Ansage-Varianten

Es sind folgende Ansage-Varianten verfügbar:

- Begrüßungsansage (Ansage vor Melden)
  Einem Anrufer kann vor Annahme des Anrufs eine Begrüßungsansage eingespielt werden.
- AutoAttendant
  Bei aktivem AutoAttendant kann einem Anrufer Musik und/oder weitere Ansagen eingespielt werden, falls er nicht sofort vermittelt werden kann.
- MFV-Durchwahl
  Bei aktiver MFV-Durchwahl wird einem Anrufer über eine Ansage eine Durchwahlmöglichkeit angeboten. Während der Ansage ist ein Codeempfänger aktiv, der die Nachwahl des Anrufers erkennt und weiterleitet.

Alternativen zur a/b-Schnittstelle (SLA-Baugruppen)

- OpenScape Business X8: TMEW2-Baugruppe

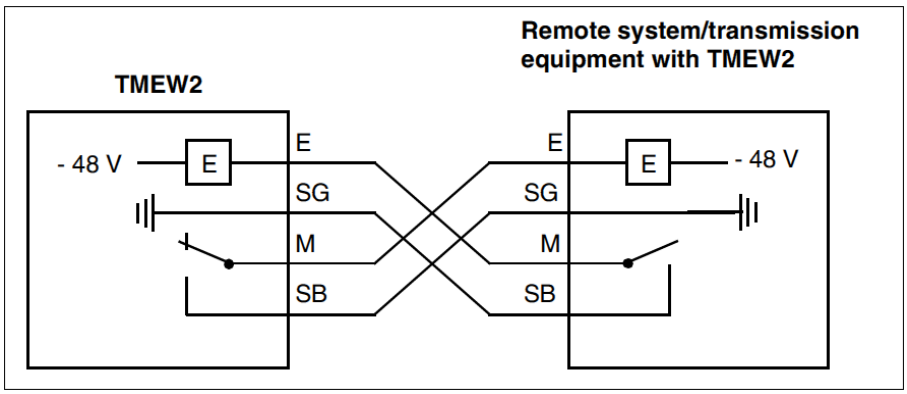
- OpenScape Business X5: STRB-Optionsbaugruppe
- OpenScape Business X3: STRBR-Optionsbaugruppe

Ansageverzögerung

Die Ansageverzögerung gibt an, nach welcher Zeit (0-600s einstellbar) ein wartender Ruf auf ein Ansagegerät weitergeschaltet wird.

Ansagegerät Genius

Für den Anschluss des Ansagegerätes Genius kann die TMEW2-Baugruppe auf Schnittstellentyp 2 eingestellt werden. Die Beschreibung zur TMEW2-Baugruppe sowie die Belegung der SIVAPAC-Stecker auf der Backplane bei Anschluss des Ansagegerätes Genius finden Sie in der Servicedokumentation, Montage der Hardware im Kapitel "Baugruppen".



Die Konfiguration des Ansagegeräts Genius erfolgt mit dem Manager E über **Anlagensicht > Einstellungen > Anschaltungen > Ansage**.

21.1.1 Wie Sie ein analoges Ansagegerät hinzufügen

Voraussetzungen

- Das Ansagegerät ist an eine analoge Schnittstelle angeschlossen.
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Endgeräte / Teilnehmer**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Analog-Endgeräte** zu starten. Es wird Ihnen eine Liste aller analogen Teilnehmer angezeigt.

4) Tragen Sie in der Zeile des Ansagegeräts Namen und Rufnummern ein.

5) Treffen Sie bei Bedarf in der Zeile des Ansagegeräts weitere Einstellungen.

6) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

21.1.2 Wie Sie die Ansageverzögerung ändern

Die Konfiguration erfolgt im Manager E (siehe auch Online-Hilfe des Manager E):

Schritt für Schritt

› **Anlagensicht**, Menü **Einstellungen > Systemparameter > Zeitparameter**: in der Tabelle bei dem Eintrag **Verzögerungszeit bis zur Ansage vor Melden aus** die **Basis** und den **Multiplikationsfaktor** der Ansageverzögerung an die eigenen Wünsche anpassen (Standard: 100ms x 20).

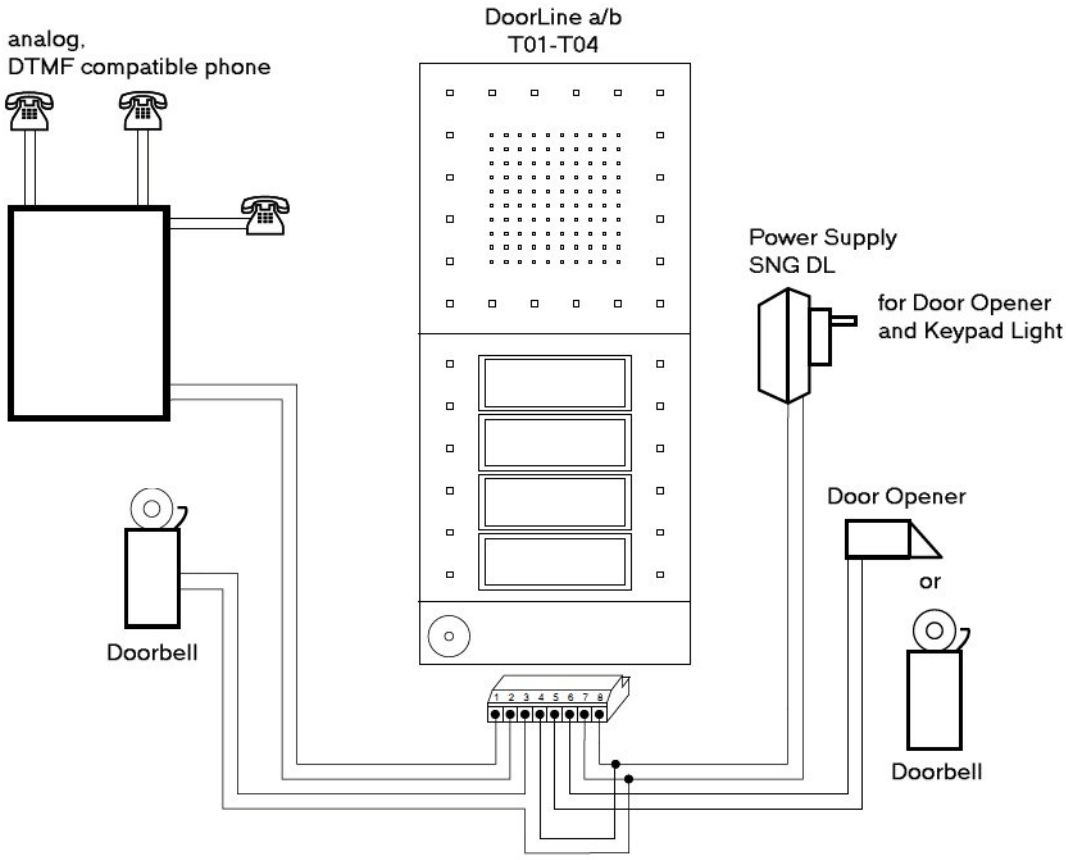
21.2 Türsprechstelle und Türöffner

Türsprechstellen (TFE) werden heute in einer vielfältigen Auswahl von diversen Herstellern angeboten. Dabei sind die Anschlussvarianten ausschlaggebend für die Bedienung und die Funktionalität einer jeden TFE. Beispielhaft ist hier die Doorline a/b T01-T04 beschrieben, wobei sich Türsprechstellen von Behnke, Keil, 2n EntryCom, Auerswald, etc ähneln.

21.2.1 DoorLine a/b T01-T04

Die Türsprechstelle DoorLine a/b T01-T04 wird an eine analoge Schnittstelle angeschlossen. Ausgerüstet mit 1 bis 4 Klingeltastern (je nach Ausführung) können mehrere unabhängige Wohn- und Geschäftsbereiche erreicht werden. Sie kann aber nicht nur von jedem Telefon aus bedient werden, sondern bietet darüber hinaus auch den Anschluss für die Stromversorgung des Türöffners.

Durch die 2-Draht-a/b-Technik ist die DoorLine a/b T01-T04 schnell und einfach zu montieren. Für die Abstimmung zum Kommunikationssystem kann das Wahlverfahren eingestellt und der Sprechweg abgeglichen werden. Die Türöffnung erfolgt über Kennziffer der Doorline (z.B. #9). Ein spezielles Anschaltmodul wie Doorline M02, M03, M06 und M06/1 ist nicht mehr notwendig.



INFO: Für dies Türsprechstelle ist keine weitere Einstellung in OpenScape Business notwendig. Aus Sicherheitsgründen empfiehlt es sich, die Nebenstelle als "Nichtamt" oder als "Halbamt" zu konfigurieren.

21.2.1.1 Wie Sie den Teilnehmerport der Doorline a/b T01-T04 konfigurieren

Die Konfiguration erfolgt im Manager E (siehe auch Online-Hilfe des Manager E):

Schritt für Schritt

1) **Anlagensicht**, Menü **Einstellungen > Station einrichten > Teilnehmer**: für den Teilnehmerport den Typ **Standard** auswählen.
2) **Teilnehmersicht**, Registerkarte **Flags**: für den Teilnehmerport das Flag **Anklopfschutz ein** aktivieren.
3) **Anlagensicht**, Menü **Einstellungen > Systemparameter**, Registerkarte **Flags**: das Flag **DTMF automatisch** aktivieren.

21.2.1.2 Wie Sie die Nebenstelle für die Doorline a/b T01-T04 konfigurieren

Die Konfiguration erfolgt im Manager E (siehe auch Online-Hilfe des Manager E):

Schritt für Schritt

1) **Teilnehmersicht**, Registerkarte **Flags**: für die Nebenstelle das Flag **Anklopfschutz ein** deaktivieren.
2) **Teilnehmersicht**, Registerkarte **Flags**: für die Nebenstelle das Flag **Anruferliste ausgeben** aktivieren.

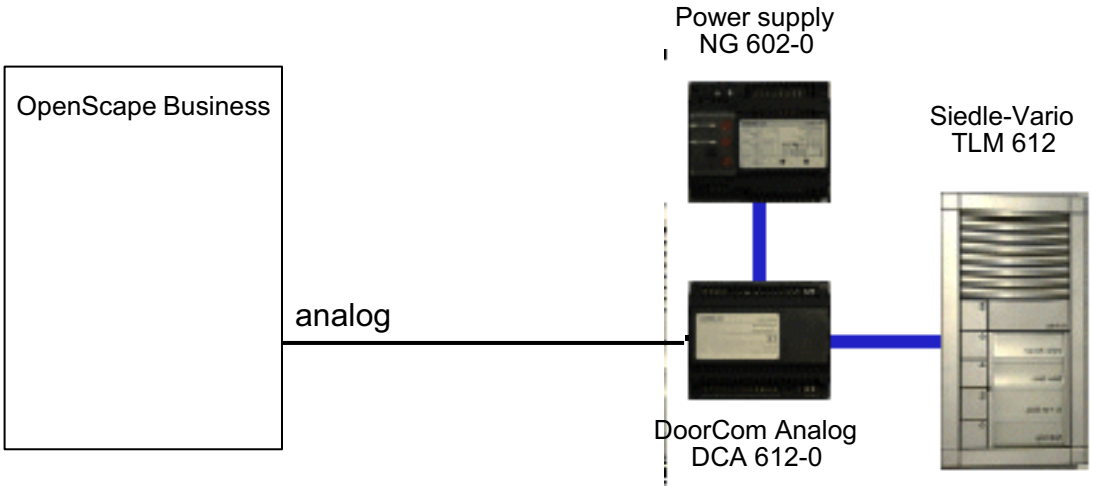
21.2.2 DoorCom Analog

Bei der DoorCom® Analog handelt es sich um eine universelle TFE-Adapterbox für die Tür- und Torsprechstellen der Firma Siedle (zum Beispiel Vario TLM 612).

Die DoorCom® Analog wird an eine analoge Schnittstelle des Kommunikationssystems angeschlossen. Sie verhält sich wie ein analoges Telefon mit MFV-Wahl, MFV-Erkennung und MFV-Steuerung. Die Steuerung ist nur über MFV-Zeichen möglich.

DoorCom Analog ist ausschließlich in Verbindung mit folgenden Komponenten funktionsfähig:

- DoorCom Analog DCA 612-0
- Tür- und Torsprechstelle Siedle-Vario TLM 612
- Schalt-Fernsteuer Interface DCSF 600
  Für die Sprachverbindung von einem internen Teilnehmer zur Tür- und Torsprechstelle. Ohne dieses Modul ist kein Zurückrufen der Tür- und Torsprechstelle möglich, z. B. wenn ein Anruf von der Tür- und Torsprechstelle versehentlich ausgelöst wurde.
- Netzteil NG 602-0



Es besteht die Möglichkeit, die Steuerfunktionen des Gerätes (Tür öffnen, Türsprechstelle anwählen, ...) auf die Prozedurtasten eines Telefons zu programmieren. Die dort gespeicherte MFV-Zeichenfolge wird dann zur Türsprechstelle/ Türöffner gesendet.

INFO: Für dies Türsprechstelle ist keine weitere Einstellung in OpenScape Business notwendig. Aus Sicherheitsgründen empfiehlt es sich, die Nebenstelle als "Nichtamt" oder als "Halbamt" zu konfigurieren.

21.2.2.1 Wie Sie den Teilnehmerport der DoorCom Analog konfigurieren

Die Konfiguration erfolgt im Manager E (siehe auch Online-Hilfe des Manager E):

Schritt für Schritt

1) **Anlagensicht**, Menü **Einstellungen > Station einrichten > Teilnehmer**: für den Teilnehmerport den Typ **Standard** auswählen.
2) **Teilnehmersicht**, Registerkarte **Flags**: für den Teilnehmerport das Flag **Anklopfschutz ein** aktivieren.
3) **Anlagensicht**, Menü **Einstellungen > Systemparameter**, Registerkarte **Flags**: das Flag **DTMF automatisch** aktivieren.

21.2.2.2 Wie Sie die Nebenstelle für die DoorCom Analog konfigurieren

Die Konfiguration erfolgt im Manager E (siehe auch Online-Hilfe des Manager E):

Schritt für Schritt

1) **Teilnehmersicht**, Registerkarte **Flags**: für die Nebenstelle das Flag **Anklopfschutz ein** deaktivieren.

2) **Teilnehmersicht**, Registerkarte **Flags**: für die Nebenstelle das Flag **Anruferliste ausgeben** aktivieren.

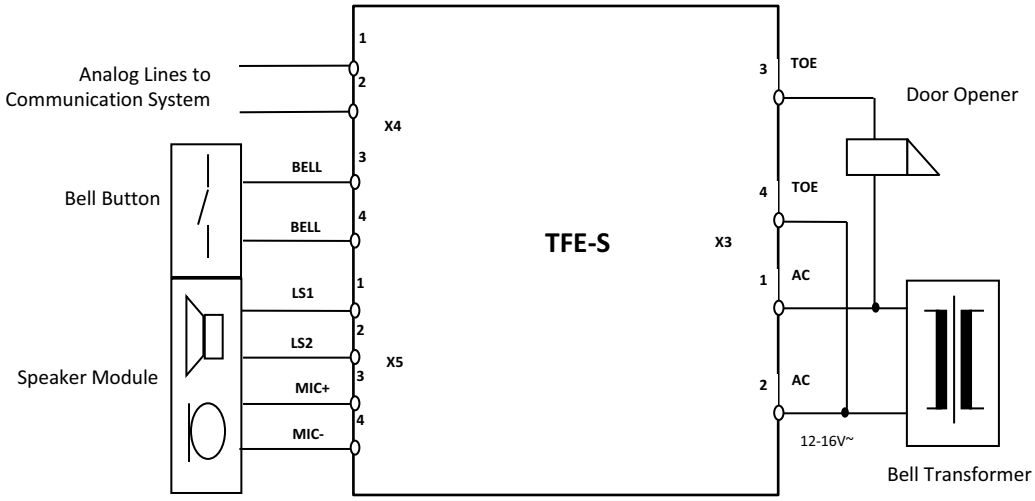
21.2.3 Türfreisprecheinrichtung mit Verstärker (TFE-S)

Das TFE-S Modul (S30122-K7696-T313) verbindet eine analoge Schnittstelle des Kommunikationssystems mit einer Türfreisprecheinrichtung, einem Türöffner und einem Klingeltaster. Die Steuerung erfolgt über das Kommunikationssystem.

Damit ist ein Anschluss an passive Türsprechstellen möglich, die mit folgenden Typen vergleichbar sind:

- Fa. Siedle (TLM511-01, 611-01)
- Fa. Rito (5760)
- Fa. Grothe (TS6216)

Die Verstärkung ist manuell einstellbar. Das TFE-S-Modul benötigt eine eigene Stromversorgung.



Technische Daten

Parameter	Wert
Stromversorgung	Klingeltrafo 12V - 16V AC, 50Hz
Stromaufnahme	max. 150mA

Parameter	Wert
Schnittstelle OpenScape Business	analoger Teilnehmer
Abmessungen	100mm x 160mm
Umgebungstemperatur	0°C bis +45°C

Funktionsbeschreibung

Das Betätigen der Türklingel wird einem definierten Teilnehmer (Türrufzielstelle) an seinem Telefon als Anruf signalisiert. Nimmt der Teilnehmer den Anruf an, wird eine Sprechverbindung zur Türsprechstelle aufgebaut. Zusätzlich kann der Teilnehmer an seinem Telefon den Türöffner aktivieren.

Wenn die Türrufzielstelle nicht erreichbar ist, erfolgt ein Abwurf. Ist die Abwurfstelle nicht frei, erfolgt ein Systemsuchlauf über alle Systemtelefone.

INFO: Bei der Signalisierung eines Türrufs wird die Nachtschaltung nicht berücksichtigt.

INFO: KWZ ist an der Türsprechstelle nicht nutzbar.

Konfigurationsmöglichkeiten

Folgende Konfigurationsmöglichkeiten stehen zur Verfügung:

- Türöffner:
  Der Türöffner wird über eine a/b-Schnittstelle eingerichtet. Hierfür muss an der Türsprechstelle eine Adapterbox angeschaltet werden. Der Teilnehmer kann dadurch die Tür, durch einen einfachen Tastendruck am Telefon, während der Verbindung mit der Türstelle öffnen.
- MFV (DTMF):
  Hier wird festgelegt, ob der Türöffner mit einem MFV-Sender aktiviert wird (MFV: Mehrfrequenzwahlverfahren), d. h. die Türrufzielstelle kann die Tür durch MFV-Nachwahl öffnen.
- Anrufumleitung (AUL):
  Hier wird festgelegt, ob der Ruf von der Türsprechstelle einer externen Anrufumleitung der Zielstelle folgen soll.

21.2.3.1 Wie Sie die Türsprechstelle konfigurieren

Mit dem Wizard **Türsprechstelle** können Sie festlegen, welche Teilnehmer den Türöffner betätigen können.

Voraussetzungen

- Sie sind am WBM angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Zentrale Telefonie**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Türsprechstelle** zu starten. Das Fenster **Türsprechstelle ändern** wird angezeigt.

4) Wählen Sie eine bzw. mehrere **Sprechstellen** aus.

5) Geben die **Zielstelle** ein.

6) Aktivieren Sie im Kontrollkästchen die zugehörigen Funktionen wie **Türöffner**, **DTMF** und **AUL**.

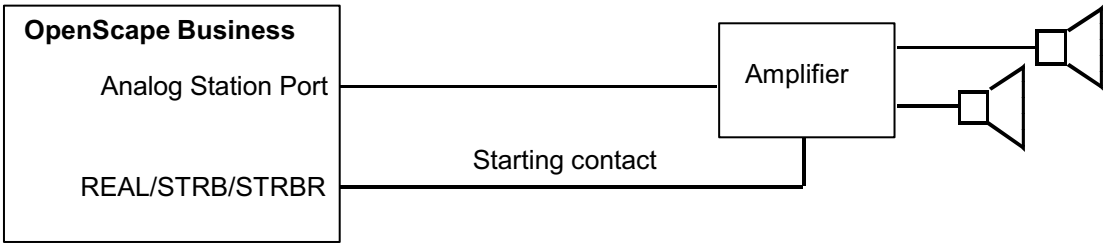
7) Klicken Sie auf **OK & Weiter** und abschließend auf **Beenden**.

21.2.4 Lautsprecher

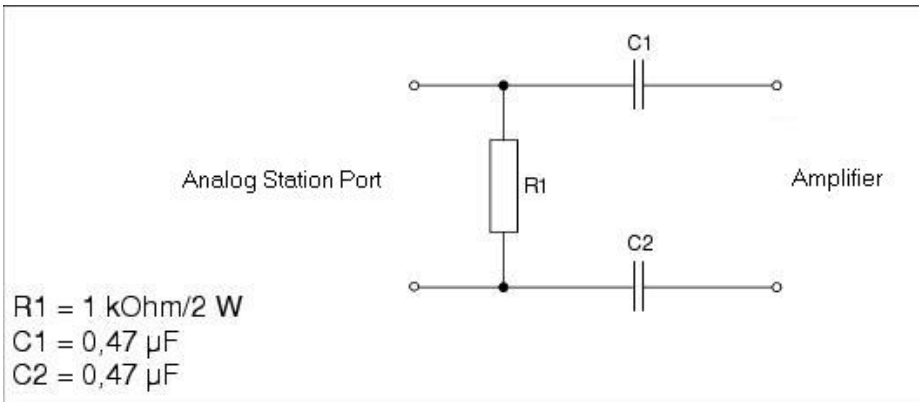
Lautsprecher können über Verstärker an das Kommunikationssystem angeschlossen werden.

Für den Anschluss eines Verstärkers inkl. Lautsprecher bestehen folgende Möglichkeiten:

- **Anschluss des Verstärkers an eine analoge Teilnehmer-Schnittstelle**
  Evtl. ist hierfür eine Pegelanpassung des Verstärkers erforderlich.



Evt. ist zusätzlich ein Schleifenwiderstand nach folgender Schaltung zu verwenden:



- **Anschluss des Verstärkers an das TFE S Modul**
  Ein ein aktiver Verstärker/ Verstärkeranlage lässt sich über das TFE S Modul anschalten. Der Verstärkereingang wird an den Lautsprecherausgang des TFE S Modules angeschlossen.
  Evt. ist noch ein Kontakt der STRB-Baugruppe erforderlich, um den Verstärker einzuschalten oder das Eingangssignal durchzuschalten (Unterdrückung von Störgeräuschen).

21.2.4.1 Wie Sie die analoge Teilnehmer-Schnittstelle für einen Lautsprecher konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Teilnehmer**.

3) Klicken Sie im Menübaum auf **Teilnehmer > Analoge Teilnehmer**.

4) Wählen Sie den gewünschten analogen Teilnehmer aus (z. B. 3011).

5) Ändern Sie in der Registerkarte **Teilnehmer-Parameter ändern** die Daten des analogen Teilnehmers wie benötigt.

6) Wählen Sie in der Aufklappliste **Stationstyp** den Eintrag **Lautsprecher** aus.

7) Klicken Sie auf **Übernehmen**.

21.2.4.2 Wie Sie die analoge Teilnehmer-Schnittstelle für den Anschluss eines Verstärker am TFE S Modul konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Zentrale Telefonie**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Türsprechstelle** zu starten. Das Fenster **Türsprechstelle ändern** wird angezeigt.

4) Wählen Sie eine **Sprechstelle** aus.

5) Wählen Sie die **Zielstelle** aus.

6) Klicken Sie auf **OK & Weiter** und abschließend auf **Beenden**.

21.3 Aktoren

Aktoren sind Steuerausgänge und werden durch Steuersignale des Kommunikationssystems aktiviert oder deaktiviert. Sie bewirken eine Zustandsänderung der angeschalteten Einrichtung und unterstützen Funktionen zum Überwachen, Alarmieren, Steuern und Regeln. Sie werden hauptsächlich in Sicherheits- und Hausverwaltungssystemen eingesetzt (z. B. für Türöffner).

Aktoren sind auf optionalen Steuerrelais-Baugruppen enthalten. Alle Steuerrelais-Baugruppen enthalten 4 Steuerausgänge (Aktoren).

Mögliche Steuerrelais-Baugruppen:

- REALS (OpenScape Business X8)
- STRB (OpenScape Business X3W/X5W)
- STRBR (OpenScape Business X3R/X5R)

Die genaue Beschreibung dieser Baugruppen inkl. der Belegungen finden Sie in der Servicedokumentation im Kapitel "Baugruppen".

Für die Steuerung der Aktoren gibt es folgende Möglichkeiten:

- vom Telefon aus über Kennzahlen
- vom Systemtelefon aus über eine Taste
- per Fernzugriff über die Amtsleitung (DISA) durch den der Relaisfunktion zugewiesenen Teilnehmer
- per Fernzugriff über das Leistungsmerkmal "Assoziierte Dienste"

Aktoren können durch folgende Funktionen aktiviert oder deaktiviert werden:

> ***INFO:*** Die Kennzahlen für die Steuerung finden Sie im Kapitel "Experten-Modus".

- **Ohne Funktion**
  Der Aktor ist entweder nicht in Betrieb oder als zentraler Wecker eingetragen (unter "Einstellungen" - "Kommende Rufe" - "Rufziellisten").
- **Manuell ein und aus**
  Der Aktor kann über Taste oder Kennzahl "Ausgewählter Schalter ein- bzw. ausschalten" aktiviert oder deaktiviert werden. Diese Funktion kann einem Teilnehmer, einer Gruppe oder alle Teilnehmer zugewiesen werden.
- **Autom. nach Zeit aus**
  Der Aktor kann als Zeitschalter über Taste oder Kennzahl "Ausgewählter Schalter ein- bzw. ausschalten" aktiviert oder deaktiviert werden. Diese Funktion kann einem Teilnehmer, einer Gruppe oder alle Teilnehmer zugewiesen werden. Wird als Schaltzeit ein Wert größer als 0 eingegeben, wird der Aktor erst nach Ablauf dieser Schaltzeit deaktiviert.
- **Türöffner**
  Der Aktor kann als Türöffner über Taste oder Kennzahl "Ausgewählter Schalter ein- bzw. ausschalten" aktiviert oder deaktiviert werden. Diese Funktion kann einem Teilnehmer, einer Gruppe oder alle Teilnehmer zugewiesen werden. Wird als Schaltzeit ein Wert größer als 0 eingegeben,

wird der Aktor erst nach Ablauf dieser Schaltzeit deaktiviert. Allen zugeordneten Endgeräten wird im Display der Text “Türöffner” angezeigt. Beispiel für den Faktor der Schaltzeit: 30*100ms = 3 sec.

- **Lsp.-Verstärker**
  Der Aktor wird aktiviert, wenn eine Verbindung zur Türsprechstelle/Torstelle/Lautsprecherbox aufgebaut wird. Er wird deaktiviert, sobald die Verbindung getrennt wird. Hiermit kann ein Türsprechstellenverstärker gesteuert werden, damit dieser nur im Bedarfsfall eingeschaltet wird. Dieser Funktion muss die Türsprechstelle oder der Lautsprecherport zugeordnet werden.
- **Besetztanzeige**
  Der Aktor wird aktiviert, wenn der zugeordnete Teilnehmer den Ruhezustand verlässt (Hörer abgenommen oder Lautsprecher aktiviert oder Endgerät des Teilnehmers wird angerufen). Der Aktor wird deaktiviert, wenn sich der zugeordnete Teilnehmer wieder im Ruhezustand befindet. Der Aktor kann auch direkt über Taste oder Kennzahl "Ausgewählter Schalter ein- bzw. ausschalten" oder eine Taste aktiviert werden. In diesem Fall wird der Status des zugeordneten Teilnehmers ignoriert und der Aktor kann nur mittels Taste oder Kennzahl wieder deaktiviert werden. Dieser Funktion muss ein bestimmter Teilnehmer zugeordnet werden. Beispiel Türbesetztanzeige: Telefoniert der Chef, geht eine Lampe über der Türe des Chefs an, die signalisiert, dass der Chef nicht gestört werden will.
- **Halten-Musik**
  Der Aktor wird aktiviert, wenn sich mindestens ein Teilnehmer oder eine Leitung des Kommunikationssystems nicht im Ruhezustand befindet. In diesem Fall wird ein Ansagegerät oder ein CD-Player aktiviert. Der Aktor wird deaktiviert, wenn alle Teilnehmer und Leitungen des Kommunikationssystems sich im Ruhezustand befinden. Dieser Funktion kann nur allen Teilnehmern zugeordnet sein und darf nur einmal im Kommunikationssystem vorhanden sein. Als Schaltzeit muss ein Wert größer als 0 eingegeben werden (z. B. 600*100ms = 60 sec). Der Aktor ist so lange aktiv und spielt Musik, bis die Schaltzeit abgelaufen ist oder der Aktor per Steuersignal deaktiviert wird.
- **Zweitwecker**
  Der Aktor wird für den zugeordneten Teilnehmer aktiviert, wenn dieser angerufen wird. Mit dem Melden bzw. Rufende wird der Aktor wird deaktiviert. Der Aktor ist nicht getaktet. Dieser Funktion muss ein bestimmter Teilnehmer zugeordnet werden. Wird als Schaltzeit ein Wert größer 0 eingegeben, wird eine Ausschalteverzögerung erreicht. Die Schaltzeit ist ein Vielfaches von 3 Sekunden.
- **Gebühren-Impuls**
  Der Aktor wird anhand der eintreffenden Gebührenimpulse oder Gebührenmeldung(en) entsprechend der Anzahl für den zugeordneten Teilnehmer getaktet. Dieser Funktion muss ein bestimmter Teilnehmer zugeordnet werden. Die Schaltzeit ist mit 150 ms Puls und 150 ms Pause nicht änderbar.
- **Teilnehmer aktiv**
  Der Aktor wird aktiviert, wenn der zugeordnete Teilnehmer aktiv ist (Hörer abgenommen oder Lautsprecher aktiviert). Der Aktor wird deaktiviert, wenn sich der zugeordnete Teilnehmer wieder im Ruhezustand befindet. Dieser Funktion muss ein bestimmter Teilnehmer zugeordnet werden.

Aktornamen

Den Aktoren können beliebige Namen (max. 16 Zeichen) zugewiesen werden.

21.3.1 Wie Sie einen Aktor konfigurieren

Voraussetzungen

- Eine Steuerrelais-Baugruppe ist gesteckt.

Die Konfiguration erfolgt im Manager E (siehe auch Online-Hilfe des Manager E):

Schritt für Schritt

1) **Anlagensicht**, Menü **Einstellungen > Anschaltungen > Aktoren**: unter **Aktoren-Liste** den zu konfigurierenden Aktor auswählen.

2) **Anlagensicht**, Menü **Einstellungen > Anschaltungen > Aktoren**: unter **Aktor-Typ** die Funktion für den Aktor auswählen.

3) **Anlagensicht**, Menü **Einstellungen > Anschaltungen > Aktoren**: im Feld **Aktor-Name** einen frei wählbaren Namen für den Aktor eingeben (max. 16 Zeichen).

4) Wenn der Funktion ein Teilnehmer, eine Gruppe oder alle Teilnehmer zugeordnet werden sollen, ist im Bereich **zugeordneter Teilnehmer** in der Liste **Rufnummer** die Rufnummer des Teilnehmers oder die Gruppenrufnummer auszuwählen.

Für alle Teilnehmer ist der Eintrag **keine** auszuwählen.

5) Wenn die Funktion eine Schaltzeit erfordert, ist im Bereich **Schaltzeit** im Feld **Faktor** der Faktor einzugeben, der mit dem angezeigten Wert multipliziert wird.

Mögliche angezeigte Werte sind 100ms und 3s.

21.4 Sensoren

Sensoren sind Steuereingänge und erkennen eine Zustandsänderung der angeschalteten Einrichtung. Sie können Funktionen des Kommunikationssystems aktivieren oder deaktivieren und unterstützen somit Funktionen zum Überwachen, Alarmieren, Steuern und Regeln. Sie werden hauptsächlich in Sicherheits- und Hausverwaltungssystemen eingesetzt (z. B. für Temperaturüberwachung oder Bewegungsmelder).

Sensoren sind auf optionalen Steuerrelais-Baugruppen enthalten. Alle Steuerrelais-Baugruppen enthalten 4 Steuereingänge.

Mögliche Steuerrelais-Baugruppen:

- REALS (OpenScape Business X8)
- STRB (OpenScape Business X3W/X5W)
- STRBR (OpenScape Business X3R/X5R)

Die genaue Beschreibung dieser Baugruppen inkl. der Belegungen finden Sie in der Servicedokumentation im Kapitel "Baugruppen".

Sensoren können folgende Funktionen aktivieren oder deaktivieren:

> ***INFO:*** Die Kennzahlen für die Steuerung finden Sie im Kapitel "Experten-Modus".

- Rufsignalisierung an Telefonen
- Displaymeldung an Systemtelefonen
- Ein-/Ausschalten eines Ansagegerätes
- Steuerung eines Anrufbeantworters
- Automatische Wahl mit einer vordefinierten Rufnummer (interne Rufnummer, Gruppenrufnummer oder externe Zielrufnummer)
- Aktivierung der folgenden Dienste für eine Rufnummer (mit Code + Rufnummer):
  - Aktor ein-/aus
  - Anrufschutz ein/aus
  - Anrufumleitung ein/aus
  - Codeschloss ein/aus
  - Mitteilungstexte senden
  - Mitteilungstexte zurückziehen
  - Nachtbetrieb ein/aus
  - Rufübergabe ein/aus
- Direkte Aktivierung folgender Dienste (nur mit Rufnummer):
  - Aktor ein-/aus
  - Kurzwahlsystem verwenden
- Fehlersignalisierung - möglich ist
  - die Ausgabe einer programmierbaren Fehlermeldung (Sensorname, max. 10 Zeichen: z. B. Temp-Alarm) am Display eines bestimmten Systemtelefons (keine akustische Signalisierung).
  - der Anruf bei einem bestimmten Systemtelefon mit Fehlermeldung im Display während des Anrufs (Zielrufnummer)
  - ein Fehlereintrag in der Error History (Eintrag im Fehlerspeicher = aktivieren)

Zielrufnummer

Ein zugeordneter analoger Port ist für die Sensoren programmierbar. Dieser Port wird vom System gerufen, sobald ein Verbindungsaufbausignal empfangen wird. Der rufende Teilnehmer umgeht daraufhin diesen Anschluss. Wenn an den betreffenden Port eine Ansageeinrichtung angeschlossen ist, kann eine Sprachansage eingespielt werden, die den gerufenen Teilnehmer über das Ansprechen des Sensors informiert. Ein auf diese Weise programmierter analoger Port kann von außerhalb nicht angesprochen werden. Wurde für einen Sensor eine externe Rufnummer programmiert, für einen analogen Port jedoch nicht, dann wird die externe Verbindung zwar hergestellt, aber kein akustisches Signal im Zusam-

menhang mit dem Ansprechen des Sensors übermittelt. Erforderlichenfalls kann der gerufene Teilnehmer jedoch anhand der Rufnummer (CLIP) den Ursprung des Anrufs feststellen.

Steuerdateneingabe

Eingabe der Steuerzeichenkette mit maximal 24 Zeichen für das Phonemail-System (Briefkasten-Rufnummer). Sobald die Verbindung hergestellt ist, wird die Steuerzeichenkette an den Ansage-Port übermittelt. Ist kein Ansage-Port verfügbar, wird die Steuerzeichenkette an das Ziel übertragen.

21.5 OpenStage Gate View

OpenStage Gate View ist eine benutzerfreundliche Sicherheits-Einstiegslösung, die in Echtzeit Videobilder auf Ihrem OpenStage Telefon, dem PC oder – unterwegs – auf dem iPhone bereitstellt.

So können Sie Ihren Eingangsbereich überwachen, kontrollieren und den sicheren Zutritt auf Ihr Unternehmensgelände gewähren.

Die wichtigsten Bedienschritte für den Anwender von OpenStage Gate View an einem OpenStage 60/80, an einem iPhone oder an einem Web Client sind in der *Kurzbedienungsanleitung* beschrieben.

21.5.1 Rechtliche Rahmenbedingungen

Videoüberwachung ist die Beobachtung von Orten durch optisch-elektronische Einrichtungen, auch optische Raumüberwachungsanlage genannt. Beim Einsatz von Videoüberwachung sind die landesspezifischen Vorschriften und Gesetze zu beachten.

Länderspezifische Rechtssituation

Die Videoüberwachung öffentlich zugänglicher Räume wird in den Ländern unterschiedlich gehandhabt. Erkundigen Sie sich deshalb nach den rechtlichen Rahmenbedingungen in Ihrem Land.

Falls eine Videoüberwachung stattfindet, kann es sein, dass der überwachte Bereich durch ein Symbol gekennzeichnet sein muss. Ein entsprechendes Symbol wird vom Kamerahersteller in der Regel mitgeliefert und kann wie folgt aussehen.



21.5.2 Komponenten

Zur Verwendung von OpenStage Gate View werden die Komponenten *Quelle*, *Verarbeitung* und *Darstellung* benötigt. Alle Komponenten werden durch ein lokales Netzwerk miteinander verbunden.

Quelle

Die Videoquelle stellt das Videosignal bereit. Als Quelle können Kameras verschiedener Hersteller verwendet werden. Abhängig vom Kamera-Typ kann zusätzlich ein Videokonverter erforderlich sein.

- IP-Kameras
- Analog-Kameras (in Kombination mit Composite/IP-Konverter)
- Türsprechstellen mit integrierter Kamera

Die Schnittstelle zur Weiterverarbeitung des Videosignals ist immer ein IP-Videostream.

Wird als Videoquelle eine handelsübliche Netzwerk-Kamera verwendet, wird zum Anschluss der Kamera unter Umständen ein LAN mit Power over Ethernet (PoE) benötigt.

Verarbeitung

Zur Verarbeitung des Videosignals ist eine Serversoftware erforderlich, die bereits im Kommunikationssystem integriert ist. Es ist keine weitere Hardware zur Verarbeitung des Videosignals erforderlich

Darstellung

Die Darstellung ist an verschiedenen Endgeräten möglich. Folgende Geräte sind zur Darstellung des Videosignals vorgesehen.

- Geräte der OpenStage Familie ab Version V2R0.48.0.
  - OpenStage 60/80 HFA
  - Octophon 660/680 HFA
- iPhone
  Mithilfe der iPhone App *OpenStage Gate View*, erhältlich im Apple AppStore.
- Webbrowser
  Darstellung innerhalb der web-basierten Administrationssoftware *Video Surveillance System* oder als Web-Client.

Von einigen Geräten aus lässt sich die Aufzeichnung des Videosignals am Server steuern.

21.5.3 Funktionsübersicht

OpenStage Gate View ermöglicht durch Verwendung eines OpenStage 60/80 HFA Telefons die Kombination aus bester Sprachqualität, Videoübertragung und Türöffner-Funktion an einem Endgerät.

Funktionen und Vorteile

- Video-Aufzeichnung auf Netzwerk-Laufwerk.
- Unterschiedliche Darstellung mehrerer Video-Signale an OpenStage-Telefonen, Mobiltelefonen (iPhone App) oder Web-Clients.
- Einfache, passwortgeschützte Administration per web-basierter, mehrsprachiger Oberfläche.
- Flexibles Lizenzierungskonzept.
- Integriert sich in schon getätigte Investitionen (Geräte und Infrastruktur).

Ausbaugrenzen

Abhängig von der Plattform, auf der die Server-Software läuft, können unterschiedlich viele Kameras und Geräte zur Darstellung eingesetzt werden.

- Hardwareplattform:
  - 2 Kameras
  - 10 OpenStage-Telefone
  - 10 iPhones oder Web-Clients
- Softswitch / Application Server:
  - 8 Kameras
  - 20 OpenStage-Telefone
  - 10 iPhones oder Web-Clients

Darüber hinaus ist die maximale Anzahl einsetzbarer Kameras von den erworbenen Lizenzen abhängig. Eine Lizenz entspricht hierbei einer Kamera.

21.5.4 Menü

Dieser Abschnitt gibt einen Überblick über das Menü der Administrationssoftware und beschreibt die Einrichtung einzelner Leistungsmerkmale und Parameter.

Nachfolgend eine Übersicht der Menüfunktionen.

Übersicht

Zeigt Detailinformationen zu jeder installierten Kamera mit Bearbeitungsmöglichkeiten.

Überwachung

Zeigt das Videobild zu jeder installierten Kamera.

Aufzeichnung

Ermöglicht die Konfiguration verschiedener Parameter zur Aufzeichnung des Videobildes.

Status

Zeigt Informationen zur Hard- und Software des OpenStage Gate View Systems.

Administration

- **Verwaltung**
  Ermöglicht das Löschen von Software- und Benutzer-Daten.
- **Konfiguration der Aufnahme**
  Ermöglicht die Konfiguration des Aufnahmegerätes und der Aufnahmeart.
- **Türsprechstelle**
  Ermöglicht die Konfiguration einer Türsprechstelle mit Zuordnung von Kamera und Telefon.
- **Benutzerverwaltung**
  Bietet Informationen und Einstellmöglichkeiten zu Benutzer, Profile und Sitzungen.
- **Kameras**
  - **Installierte Kameras**
    Zeigt als Liste alle installierten Kameras.
  - **Kamera hinzufügen (Erkannte)**
    Zeigt als Liste alle erkannten Kameras zum automatischen Installieren einer Kamera.
  - **Kamera hinzufügen (Manuell)**
    Ermöglicht das manuelle Installieren einer Kamera.
  - [Name der Kamera]:
    Zeigt Detailinformationen zur gewählten Kamera mit Bearbeitungsmöglichkeiten.
- **Telefone**
  - **Installierte Telefone**
    Zeigt als Liste alle installierten Telefone.
  - **Telefon hinzufügen (Erkannte)**
    Zeigt als Liste alle erkannten Telefone zum automatischen Installieren eines Telefons.
  - **Telefon hinzufügen (Manuell)**
    Ermöglicht das manuelle Installieren eines Telefons.
  - [Name des Telefons]
    Zeigt Detailinformationen zum gewählten Telefon mit Bearbeitungsmöglichkeiten.
- **Log**
  - **Logdatei ansehen**
    Zeigt die aktuelle Logdatei mit Download-Möglichkeit.
  - **Logdatei downloaden**
    Lädt die aktuelle Logdatei herunter.

21.5.5 OpenStage Gate View Ersteinrichtung

Am OpenStage Gate View Server ist eine Minimalkonfiguration erforderlich, um die Kamera und das Anzeigegerät einzurichten. Die Einrichtung ist im Normalfall in wenigen Minuten erledigt. Abhängig von der LAN-Infrastruktur und der verwendeten Komponenten können zusätzliche Installationsschritte erforderlich sein.

- Zunächst wird eine Kamera und ein Telefon zu der Server-Konfiguratioon zugeordnet.
- Danach erhält ein OpenStage 60/80 Telefon die zur Darstellung des Videobildes erforderliche Software und wird zur Bedienung der Videofunktion eingerichtet.

Falls die automatische Erkennung von Kamera oder OpenStage 60/80 Telefon fehlschlägt, haben Sie auch die Möglichkeit, diese Geräte manuell zur Konfiguration hinzuzufügen.

21.5.5.1 Wie Sie die Server-Software erstmals starten

Die OpenStage Gate View Server-Software ist bereits im Kommunikationssystem integriert. Zum erstmaligen Start muss diese zunächst aktiviert werden.

Voraussetzungen

- Das betriebsbereite Kommunikationssystem OpenScape Business ab Version V1.
- Die Lizenz für OpenStage Gate View ist aktiviert.
- Sie sind am WBM mit dem Profil *Expert* angemeldet.

Schritt für Schritt

1) Navigieren Sie im Menü zu **Experten-Modus** > **Applikationen** > **OpenStage Gate View**.

2) Klicken Sie auf **Aktivieren** und warten Sie einige Sekunden, bis die Schaltfläche **Login** aktiv ist.

3) Klicken auf **Login**.

Es erscheint der Startbildschirm der Administrationssoftware. Sie sind über das Experten-Profil des WBM automatisch eingeloggt.

Zur Erhöhung der Sicherheit sollte das Administrator-Passwort sofort geändert werden. Diese Änderung wirkt sich nicht auf den WBM-Zugang über den Experten-Account aus.

Nächste Schritte

Ändern Sie das Administrator-Passwort.

21.5.5.2 Wie Sie Ihr Administrator-Passwort ändern

Voraussetzungen

- Sie sind am OpenStage Gate View Assistant angemeldet.

Schritt für Schritt

1) Navigieren Sie im Menü zu **Administration** > **Benutzerverwaltung**.

2) Wählen Sie bei **Benutzer** den Benutzer **admin** aus.

3) Klicken Sie auf **Benutzer laden**.

4) Geben Sie bei **Passwort** das neue Paswort ein.

5) Klicken Sie auf **Benutzer speichern**.

Das Administrator-Passwort wurde geändert.

Nächste Schritte

Fügen Sie eine Kamera hinzu.

21.5.5.3 Wie Sie eine Kamera hinzufügen

Voraussetzungen

- Eine betriebsbereite Netzwerk-Kamera als Videoquelle.
- Sie sind am OpenStage Gate View Assistant angemeldet.

Schritt für Schritt

1) Navigieren Sie im Menü zu **Administration** > **Kameras** > **Kamera hinzufügen (Erkannte)**.

2) Falls keine Kamera in der Liste angezeigt wird, klicken Sie auf **Netzwerkerkennung ausführen** und bestätigen Sie mit **OK**.

3) Klicken Sie in der Liste bei der gewünschten Kamera auf **Kamera hinzufügen**.

4) Geben Sie bei **Name** einen selbstgewählten Namen für diese Kamera ein. Erlaubte Zeichen: Groß- und Kleinbuchstaben, Ziffern und der Unterstrich.

5) Wählen Sie bei **Fabrikat** den Kameratyp aus der Liste aus.

6) Die **IP Adresse** wurde durch die Netzwerkerkennung automatisch eingetragen und sollte nicht geändert werden.

7) Geben Sie bei **Kameraport** den Standardport `80` ein.

8) Wenn erforderlich, geben Sie bei **Benutzer** den Benutzername für den Zugriff auf die Kamera ein.

9) Wenn erforderlich, geben Sie bei **Passwort** das Passwort für den Zugriff auf die Kamera ein.

10) Klicken Sie auf **Speichern**.

Die Kamera ist im OpenStage Gate View Server hinzugefügt.

Nächste Schritte

Fügen Sie ein Telefon hinzu.

21.5.5.4 Wie Sie ein Telefon hinzufügen

Voraussetzungen

- Ein betriebsbereites Telefon OpenStage 60/80 HFA oder Octophon 660/680 HFA ab Version V2R0.48.0.
- Sie sind am OpenStage Gate View Assistant angemeldet.

Schritt für Schritt

1) Navigieren Sie im Menü zu **Administration** > **Telefone** > **Telefon hinzufügen (Erkannte)**.

2) Wenn erforderlich, ändern Sie bei **Standard Telefonpasswort** das Passwort für den Zugriff auf die Telefone.

3) Falls kein Telefon in der Liste angezeigt wird, klicken Sie auf **Netzwerkerkennung ausführen** und bestätigen Sie mit **OK**.

4) Klicken Sie in der Liste beim gewünschten Telefon auf **Telefon hinzufügen**.

5) Geben Sie bei **Name** einen selbstgewählten Namen für dieses Telefon ein, zum Beispiel dessen Rufnummer. Erlaubte Zeichen: Groß- und Kleinbuchstaben, Ziffern und der Unterstrich.

6) Die **IP Adresse** wurde durch die Netzwerkerkennung automatisch eingetragen und sollte nicht geändert werden.

7) Wenn erforderlich, ändern Sie bei **Telefon Admin Passwort** das Passwort für den Zugriff auf den Administrationsbereich des Telefons (Standard: 123456).

8) Klicken Sie auf **Speichern**.

Das Telefon ist im OpenStage Gate View Server hinzugefügt.

Nächste Schritte

Richten Sie die Videofunktion am Telefon ein.

21.5.6 OpenStage Gate View Videoaufzeichnung

Mit OpenStage Gate View können Sie ein Videobild aufzeichnen, um es zeitversetzt und mehrfach anzusehen.

Speicherort

Die Aufzeichnungen werden auf einem Netzlaufwerk abgespeichert.

Wenn die Videoaufzeichnung eingerichtet ist, können Sie eine Aufzeichnung einfach vom OpenStage-Telefon aus starten und stoppen. Darüber hinaus ist eine zeitgesteuerte Aufzeichnung möglich.

Die Aufzeichnungen werden in Dateien mit folgender Namenssyntax abgelegt:
`aufzeichnungsart_datum-uhrzeit_kameraname.dateiformat`

- aufzeichnungsart:
  - SCH = scheduled recording (zeitgesteuerte Aufzeichnung)
  - MAN = manual (manuelle Aufzeichnung)
  - CYC = cyclic (zyklische Aufzeichnung)
- dateiformat: z. B. mp4 oder mpeg

Qualität und Datenmenge der Aufzeichnung

Aufzeichnungen können in unterschiedlicher Qualität erstellt werden. Aufzeichnungen mit hoher Qualität benötigen mehr Speicherplatz als Aufzeichnungen mit niedriger Qualität.

Speicherplatzbedarf: Hohe Qualität: 1 Stunde etwa 650 MByte, niedrige Qualität: 1 Stunde etwa 400 MByte.

Um auf Speichermedien den Platz für die Aufzeichnung zu begrenzen, kann der Anteil des für Aufzeichnungen vorgesehenen Speicherplatzes vorab prozentual festgelegt werden.

Bei zyklischer Aufzeichnung kann die Länge eines Zyklusses zwischen 30 und 120 Minuten eingestellt werden. Abhängig von der Größe des verfügbaren Speicherplatzes werden mehrere Dateien angelegt und dabei jeweils die ältesten wieder überschrieben.

Einschränkungen

Auch beim Einsatz mehrerer Kameras kann nur das Videobild einer Kamera gleichzeitig aufgezeichnet werden.

Eine zeitgesteuerte Aufzeichnung hat Priorität gegenüber einer manuell gestarteten und beendet diese gegebenenfalls.

Nur Aufzeichnungen im mp4-Format können direkt im Browser angesehen werden. Aufzeichnungen anderer Video-Formate müssen zunächst herunter geladen werden, um sie ansehen zu können.

Standbilder (Screenshots) können nicht direkt gespeichert werden sondern müssen später aus dem gespeicherten Video erstellt werden.

Aufzeichnungen sind nur mit Kameras bekannter Fabrikate möglich. Bei der Auswahl des Kamera-Fabrikates **andere** ist keine Aufzeichnung möglich.

21.5.6.1 Wie Sie die Videofunktion am Telefon einrichten

Um die Videofunktion an einem OpenStage 60/80 nutzen zu können, muss dieses noch konfiguriert werden. Die Funktion kann danach über die freiprogrammierbaren Sensortasten am Telefon gesteuert werden. Eine Bedienung durch ein an das Telefon angeschlossenes Key Module ist nicht möglich.

Voraussetzungen

- Ein in OpenStage Gate View installiertes Telefon OpenStage 60/80.
- Sie sind am OpenStage Gate View Assistant angemeldet.

Schritt für Schritt

1) Navigieren Sie im Menü zu **Administration** > **Telefone** > **Installierte Telefone**.
2) Klicken Sie in der Liste beim gewünschten Telefon auf **Details**.
3) Klicken Sie auf **Installieren** und bestätigen Sie mit **OK**.
4) Klicken Sie in der Liste beim zuletzt bearbeiteten Telefon auf **Tastenkonfiguration**.
5) Wählen Sie bei **Video An/Aus** unter **Mit Taste** die gewünschte Taste aus, mit der die Videofunktion ein- und ausgeschaltet werden soll und geben Sie unter **Beschriftung aktivieren** und **Beschriftung deaktivieren** jeweils passende Tastenbeschriftungen ein.
6) Wählen Sie bei **Dauervideomodus An/Aus** unter **Mit Taste** die gewünschte Taste aus, mit der die Permanentvideofunktion (Anzeige auch bei eingehenden Anrufen) ein- und ausgeschaltet werden soll und geben Sie unter **Beschriftung aktivieren** und **Beschriftung deaktivieren** jeweils passende Tastenbeschriftungen ein.
7) Wählen Sie bei **Recording On/Off** unter **Mit Taste** die gewünschte Taste aus, mit der eine Aufzeichnung gestartet und gestoppt werden soll und geben Sie unter **Beschriftung aktivieren** und **Beschriftung deaktivieren** jeweils passende Tastenbeschriftungen ein.
8) Klicken Sie auf **Speichern**.
9) Klicken Sie auf **Zum Telefon übertragen** und bestätigen Sie mit **OK**.

Die Software zur Darstellung des Videobildes ist auf dem Telefon installiert. Die Taste zur Bedienung der Videofunktion ist programmiert und passend beschriftet.

21.5.6.2 Wie Sie vorhandene Aufzeichnungen bearbeiten

Voraussetzungen

- Ein Aufzeichnungsgerät ist eingerichtet.
- Es ist mindestens eine Aufnahme vorhanden.
- Sie sind am OpenStage Gate View Assistant angemeldet.

Schritt für Schritt

1) Navigieren Sie im Menü zu **Aufzeichnungen** > **Aufnahmen**.
2) Klicken Sie auf eines der Symbole am rechten Ende der Zeile des gewünschten Videos um das Video anzusehen (nur Aufzeichnungen im mp4-Format), herunter zu laden oder zu löschen.
3) Wenn gewünscht, setzen Sie einen Haken am linken Ende der Zeile des gewünschten Videos und klicken Sie auf das Symbol unter der Liste, um die ausgewählten Videos zu löschen.

21.5.7 OpenStage Gate View Türsprechstelle

OpenStage Gate View arbeitet mit analogen Türsprechstellen zusammen. Wenn jemand an der Türe läutet, wird automatisch das Videobild der Tür-Kamera am OpenStage-Telefon angezeigt. Sie können anhand des Videobildes am Telefon entscheiden, ob die Person durch Drücken einer Taste am Telefon eingelassen wird.

Türsprechstelle in der Kommunikationsplattform einrichten

Um die Türsprechstellenfunktion in OpenStage Gate View nutzen zu können, muss zunächst, abhängig von der verwendeten Kommunikationsplattform, die Türsprechstelle in der Kommunikationsplattform eingerichtet werden.

- Einrichtung der Türsprechstelle als analoges Endgerät an einem physikalischen analogen Port der Kommunikationsplattform. Die Verwendung eines Mediatrix/AP1120-Gerätes zum Aschluss einer analogen Türsprechstelle an einen IP-Anschluss ist hierfür nicht möglich.
- Einrichtung einer Türsprechstellen-Taste am OpenStage-Telefon.
- Einrichtung des Passworts für die Türsprechstellenfunktion.

Zusammen mit OpenStage Gate View kann jeweils nur eine Türsprechstelle verwendet werden.

Weitere Informationen zum Einrichten der Funktion in der Kommunikationsplattform finden Sie in der entsprechenden Servicedokumentation.

21.5.7.1 Wie Sie die Türsprechstelle einrichten

Voraussetzungen

- In der Kommunikationsplattform ist die Funktion Türsprechstelle und die entsprechende Taste am Telefon eingerichtet.
- Die Rufnummer und das Passwort für die Türspreche sind bekannt.
- Sie sind am OpenStage Gate View Assistant angemeldet.

Schritt für Schritt

1) Navigieren Sie im Menü zu **Administration** > **Türsprechstelle** > **Türsprechstelle hinzufügen**.

2) Setzen Sie einen Haken bei **Enabled**.

3) Geben Sie bei **Name** einen Namen für die Türsprechstelle ein.

4) Geben Sie bei **Web Services Server IP** die IP-Adresse der UC Suite bzw. des UC Smart Assistant ein.

5) Geben Sie bei **Web Services Server Port** den Port des UC Smart Assistant ein.

6) Wenn gewünscht, setzen Sie bei **SSL** für eine gesicherte Verbindung einen Haken.

7) Geben Sie bei **Door Opener Station Number** die Rufnummer der Türsprechstelle ein.

8) Geben Sie bei **Door Opener UC Password** das eingerichtete Passwort für die Türsprechstellenfunktion ein.

9) Wählen Sie bei **Gate View IP Client** den Namen des in OpenStage Gate View eingerichteten Telefons zur Verwendung für die Türsprechstellenfunktion aus.

10) Wählen Sie bei **Camera** den Namen der in OpenStage Gate View eingerichteten Kamera zur Verwendung für die Türsprechstellenfunktion aus.

11) Navigieren Sie im Menü zu **Administration** > **Telefone** > **Installierte Telefone**.

12) Klicken Sie in der Liste beim zuletzt bearbeiteten Telefon auf **Tastenkonfiguration**.

13) Klicken Sie auf **Zum Telefon übertragen** und bestätigen Sie mit **OK**.

14) Klicken Sie auf **Speichern**.

Die Türsprechstellenfunktion ist eingerichtet. Beim Läuten wird das Videobild der Kamera automatisch am Telefon angezeigt. Durch Drücken der Tür-öffnen-Taste am Telefon wird die Türe geöffnet.

21.5.8 OpenStage Gate View Benutzerverwaltung

Um OpenStage Gate View personalisiert nutzen zu können, haben Sie als Administrator die Möglichkeit, zusätzlich zum Standardbenutzer **admin** weitere Benutzer einzurichten.

Durch persönliche Benutzer-Accounts haben Sie als Administrator einen besseren Überblick und mehr Sicherheit bei der Nutzung von OpenStage Gate View:

- Jeder Benutzer hat ein eigenen Account mit Benutzername und Passwort.
- Sie können Benutzer vorübergehend sperren.
- Sie können Passwortänderungen erzwingen.
- Sie sehen die Sitzungsdaten der Benutzer mit IP-Adresse und Zeitpunkt der letzten Nutzung und haben die Möglichkeit, aktive Sitzungen zu beenden.
- Mithilfe der Protokolldatei können Sie zurückliegende Aktivitäten verschiedener Benutzer erkennen.

Sie können beliebig viele Benutzer einrichten, Benutzerdaten ändern und Benutzer aus der Konfiguration dauerhaft entfernen.

21.5.8.1 Wie Sie einen Benutzer hinzufügen

Voraussetzungen

- Sie sind am OpenStage Gate View Assistant als Administrator angemeldet.

Schritt für Schritt

1. Navigieren Sie im Menü zu **Administration** > **Benutzerverwaltung**.
2. Klicken Sie auf **Benutzer hinzufügen**.
3. Geben Sie bei **Benutzername** den Namen des Benutzers ein.
4. Geben Sie bei **Passwort** und bei **Passwort (Wdh.)** das initiale Passwort für diesen Benutzer ein.
5. Klicken Sie auf **Anfrage senden**.

Der Benutzer ist eingerichtet und erscheint im Ausklapplistenfeld **Benutzer**.

21.5.8.2 Wie Sie Benutzerdaten ändern

Voraussetzungen

- Sie sind am OpenStage Gate View Assistant als Administrator angemeldet.
- Es wurde mindestens ein weiterer Benutzer hinzugefügt.

Schritt für Schritt

1. Navigieren Sie im Menü zu **Administration** > **Benutzerverwaltung**.
2. Wählen Sie bei **Benutzer** den gewünschten Benutzer aus.
3. Klicken Sie auf **Benutzer laden**.
4. Ändern Sie die Profildaten wie gewünscht.
5. Wenn Sie die Sitzung des Benutzers beenden möchten, klicken Sie auf **Sitzung beenden**.
6. Klicken Sie auf **Benutzer speichern**.

Die Benutzerdaten wurden geändert.

21.5.8.3 Wie Sie einen Benutzer löschen

Voraussetzungen

- Sie sind am OpenStage Gate View Assistant als Administrator angemeldet.
- Es wurde mindestens ein weiterer Benutzer hinzugefügt.

Schritt für Schritt

1. Navigieren Sie im Menü zu **Administration** > **Benutzerverwaltung**.
2. Wählen Sie bei **Benutzer** den gewünschten Benutzer aus.
3. Klicken Sie auf **Benutzer entfernen**.
4. Bestätigen Sie die Abfrage mit **Ja**.

Die Benutzerdaten wurden dauerhaft gelöscht.

21.5.9 OpenStage Gate View Server-Administration

Behalten Sie als Administrator den Überblick über umfangreiche Server-Informationen und löschen Sie nicht mehr benötigte Daten.

- Sie können sich sowohl die Versionsnummer der installierten Server-Software, als auch die maximale Anzahl an Geräten und Lizenzen ansehen.
- Sie haben die Möglichkeit, Telefon- und Benutzerdaten dauerhaft zu löschen.
- Sie können die Protokolldaten des OpenStage Gate View Servers ansehen und herunter laden.

21.5.9.1 Wie Sie die Administrationsoberfläche öffnen

Voraussetzungen

- OpenStage Gate View ist betriebsbereit.
- Sie kennen die IP-Adresse des OpenStage Gate View Servers.

Schritt für Schritt

1) Öffnen Sie einen Internet-Browser und geben Sie die URL mit zusätzlicher Portnummer ein: `https://[IP-Adresse des Kommunikations-systems]:8009`. Das Login-Fenster öffnet sich.

2) Geben Sie als **Benutzername** `admin` und als **Passwort** `adminpass` oder das von Ihnen geänderte Passwort ein und klicken Sie auf **Log In**.

Es erscheint der Startbildschirm der Administrationssoftware.

21.5.9.2 Wie Sie Software-Informationen anzeigen

Sie können Informationen zur Software-Version, zu den maximal verwendbaren Geräten und den verfügbaren Lizenzen anzeigen lassen.

Voraussetzungen

- Sie sind am OpenStage Gate View Assistant angemeldet.

Schritt für Schritt

› Navigieren Sie im Menü zu **Administration** > **Status**.

Die Software-Informationen werden angezeigt.

21.5.9.3 Wie Sie Serverdaten löschen

Sie können sowohl Software-Daten als auch Aufzeichnungen und die Datenbank gezielt löschen.

Voraussetzungen

- Die zum Löschen vorgesehenen Daten sind vorhanden.
- Sie sind am OpenStage Gate View Assistant angemeldet.

Schritt für Schritt

1) Navigieren Sie im Menü zu **Administration** > **Verwaltung** > **Serververwaltung**.

2) Setzen Sie wie gewünscht einen Haken bei den folgenden Optionen: **Netzwerkeinstellungen zurücksetzen**, **Datenbank löschen**, **Video SW von OpenStage Telefon(en) löschen** oder **Alle Aufzeichnungen löschen**.

3) Klicken Sie auf **Reset ausführen**.

4) Bestätigen Sie die Abfrage mit **Ja**.

Die Daten sind dauerhaft gelöscht.

21.5.9.4 Wie Sie die Protokolldatei anzeigen und abspeichern

Sie können die Protokolldatei des Servers sowohl anzeigen als auch vom Server herunterladen und lokal auf Ihrem PC abspeichern. Weitere Protokolldaten sind als Trace verfügbar.

Voraussetzungen

- Sie sind am OpenStage Gate View Assistant angemeldet.

Schritt für Schritt

1) Navigieren Sie im Menü zu **Administration** > **Log** > **Logdatei ansehen**.

2) Wenn Sie die Protokolldatei sichern möchten, klicken Sie auf **Logdatei downloaden**.

Die Protokolldatei wird angezeigt.

21.5.10 OpenStage Gate View Anpassungen

Die meisten Administrations-Tätigkeiten sind automatisiert, sodass möglichst wenige Einstellungen manuell vorgenommen werden müssen. Aufgrund der Vielzahl an unterschiedlichen LAN-Konfigurationen kann es jedoch notwendig sein, einzelnen Einstellungen von Hand vorzunehmen.

- Sie können eine Kamera manuell zur Konfiguration hinzufügen und aus dieser löschen.
- Sie können ein Telefon manuell zur Konfiguration hinzufügen und aus dieser löschen.
- Am Kommunikationssystem können Sie den gesamten OpenStage Gate View Server deaktivieren.

Kamera manuell hinzufügen

Es gibt eine große Menge an Kameratypen, bereits mit den entsprechenden Zugangsdaten hinterlegt sind. In diesem Fall muss nur der Kameratyp ausgewählt und ggf. die IP-Adresse angepasst werden.

Wenn Sie eine Axis-Kamera auswählen, muss bei dieser Kamera eine Software-Version 5.0 oder höher installiert sein.

Ist die Kamera nicht in der Liste enthalten, wählen Sie **andere** aus und geben Sie die erforderlichen Zugangsparameter Kamera-IP, Port, Benutzername und Passwort als URL ein. Das Format sieht üblicherweise so aus:
`http://<Benutzername>:<Passwort>@<Kamera-IP>:<Port>`

Alle nicht aufgeführten Kameras sollten kameraseitig wie folgt eingerichtet sein:

- MJPEG als Video-Format.
- 12 Bilder pro Sekunde.
- Auflösung 320x240 Pixel.

21.5.10.1 Wie Sie eine Kamera manuell hinzufügen

Falls das automatische Erkennen einer Kamera fehlschlägt oder nicht möglich ist, kann diese manuell hinzugefügt werden.

Voraussetzungen

- Eine betriebsbereite Netzwerk-Kamera als Videoquelle.
- Sie sind am OpenStage Gate View Assistant angemeldet.

Schritt für Schritt

1) Navigieren Sie im Menü zu **Administration** > **Kameras** > **Kamera hinzufügen (Manuell)**.

2) Geben Sie bei **Name** einen selbstgewählten Namen für diese Kamera ein. Erlaubte Zeichen: Groß- und Kleinbuchstaben, Ziffern und der Unterstrich.

3) Wählen Sie bei **Fabrikat** den Kameratyp aus der Liste aus. Wenn der Kameratyp nicht in der Liste enthalten ist, wählen Sie **andere** aus.

4) Geben Sie bei **IP Adresse** die IP-Adresse der Kamera ein.

5) Geben Sie bei **Kameraport** den Standardport `80` ein.

6) Wenn erforderlich, geben Sie bei **Benutzer** den Benutzername für den Zugriff auf die Kamera ein.

7) Wenn erforderlich, geben Sie bei **Passwort** das Passwort für den Zugriff auf die Kamera ein.

8) Haben Sie bei **Fabrikat** aus der Liste **andere** gewählt, geben Sie bei **Streaming-URL** eine gültige Sreaming-URL der Kamera ein.

9) Haben Sie bei **Fabrikat** aus der Liste **andere** gewählt, geben Sie bei **Snapshot-URL** eine gültige Snapshot-URL der Kamera ein. Dies ist erforderlich zur Nutzung an mobilen Endgeräten (iPhone).

10) Klicken Sie auf **Speichern**.

Die Kamera ist im OpenStage Gate View Server hinzugefügt.

21.5.10.2 Wie Sie eine Kamera löschen

Sie können jede Kamera gezielt aus der Konfiguration löschen.

Voraussetzungen

- Die zum Löschen vorgesehene Kamera ist vorhanden.
- Sie sind am OpenStage Gate View Assistant angemeldet.

Schritt für Schritt

1) Navigieren Sie im Menü zu **Administration** > **Kameras** > **Installierte Kameras**.

2) Klicken Sie in der Liste bei der zu löschenden Kamera auf **Löschen**.

3) Bestätigen Sie die Abfrage mit **Ja**.

Die Kamera ist dauerhaft aus der Konfiguration gelöscht.

21.5.10.3 Wie Sie ein Telefon manuell hinzufügen

Falls das automatische Erkennen eines Telefons fehlschlägt, kann dieses manuell hinzugefügt werden.

Voraussetzungen

- Ein betriebsbereites Telefon OpenStage 60/80 HFA oder Octophon 660/680 HFA ab Version V2R0.48.0.
- Sie sind am OpenStage Gate View Assistant angemeldet.

Schritt für Schritt

1) Navigieren Sie im Menü zu **Administration** > **Telefone** > **Telefon hinzufügen (Manuell)**.

2) Geben Sie bei **Name** einen selbstgewählten Namen für dieses Telefon ein, zum Beispiel dessen Rufnummer. Erlaubte Zeichen: Groß- und Kleinbuchstaben, Ziffern und der Unterstrich.

3) Geben Sie bei **IP Adresse** die IP-Adresse des Telefons ein.

4) Wenn erforderlich, ändern Sie bei **Telefon Admin Passwort** das Passwort für den Zugriff auf den Administrationsbereich des Telefons (Standard: 123456).

5) Klicken Sie auf **Speichern**.

Das Telefon ist im OpenStage Gate View Server hinzugefügt.

21.5.10.4 Wie Sie ein Telefon löschen

Sie können jedes Telefon gezielt aus der Konfiguration löschen.

Voraussetzungen

- Das zum Löschen vorgesehene Telefon ist vorhanden.
- Sie sind am OpenStage Gate View Assistant angemeldet.

Schritt für Schritt

1) Navigieren Sie im Menü zu **Administration** > **Kameras** > **Installierte Telefone**.

2) Klicken Sie in der Liste bei dem zu löschenden Telefon auf **Löschen**.

3) Bestätigen Sie die Abfrage mit **Ja**.

Das Telefon ist dauerhaft aus der Konfiguration gelöscht.

21.5.10.5 Wie Sie den OpenStage Gate View Server deaktivieren

Wenn Sie die OpenStage Gate View-Funktionen nicht mehr benötigen, können Sie die OpenStage Gate View Serversoftware im Kommunikationssystem deaktivieren.

Voraussetzungen

- Das betriebsbereite Kommunikationssystem OpenScape Business ab Version V1.
- Sie haben einen Experten-Account im WBM des Kommunikationssystems.

Schritt für Schritt

1) Öffnen Sie an einem PC im LAN das WBM des Kommunikationssystems und melden Sie sich dort an.

2) Navigieren Sie im Menü zu **Experten-Modus** > **Applikationen** > **OpenStage Gate View**.

3) Klicken Sie auf **Deaktivieren** und warten Sie einige Sekunden, bis neben der Schaltfläche **OpenStage Gate View ist deaktiviert** angezeigt wird.

OpenStage Gate View-Funktionen stehen nun nicht mehr zur Verfügung.

22 Application Connectivity

Application Connectivity unterstützt das System z. B. mit CSTA, TAPI, XMPP sowie mit Application Launcher.

22.1 CSTA

CSTA ermöglicht CSTA-Anwendungen das Monitoring und die Steuerung von Telefonie-Ressourcen.

CSTA verwendet das Transmission Control Protocol (TCP). Es besteht eine feste Verbindung. Der Verlust von Datenpaketen wird erkannt und automatisch korrigiert.

Standards

Das implementierte CSTA-Protokoll beruht auf:

- ECMA-269 Services for Computer Supported Telecommunications Applications (CSTA) Phase III
- ECMA-285ASN.1 for Computer Supported Telecommunications Applications (CSTA) Phase III
- spezifischen Erweiterungen

Voraussetzungen

Die Nutzung von CSTA erfordert für das mit CSTA-Anwendungen verbundene System entweder UC Booster (Card oder Server) oder OpenScape Business S. Die Anmeldedaten für CSTA-Anwendungen müssen im System konfiguriert sein, um die CSTA-Schnittstelle automatisch zu aktivieren. Externe CSTA-Anwendungen müssen für ihren Zugriff diese Anmeldedaten verwenden.

Leistungsmerkmale

CSTA bietet folgende Leistungsmerkmale:

- Zugriff via Ethernet LAN (TCP/IP)
- CSTA Phase III, ASN.1 codiert
- breite Palette von unterstützten Systemtelefonen und Ressourcen
- netzweites Monitoring und Steuerung aller Ressourcen in einem homogenen Netz (bei Verbindung der CSTA-Anwendungen mit dem Master-Knoten)
  Es werden nur Netze mit geschlossenem Rufnummernplan unterstützt!

Unterstützte Geräte

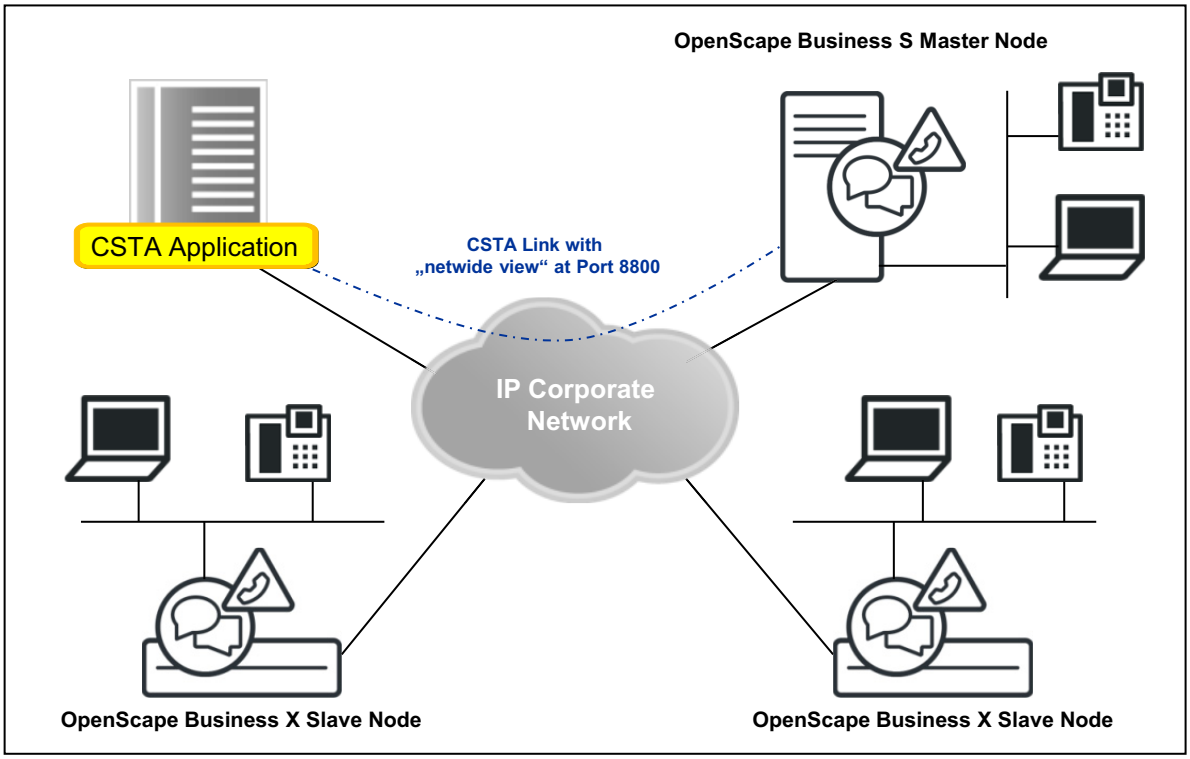
CSTA unterstützt zusätzlich zu den vom System unterstützten Telefonen folgende Geräte:

- ITSP
  ermöglicht z. B. die Nutzung von Call Center-Applikationen mit SIP-Amtsleitungen

- ISDN
- Amt analog
- virtuelle Teilnehmer
- UCD-Gruppen
- MULAPs

> ***INFO:*** Details zu Leistungsmerkmalen und unterstützten Geräten finden Sie in CSTA Interface Manual.

Anschaltung für netzweite Sicht



Ports

Folgende Portnummern stehen standardmäßig zur Verfügung:

Port	Portnummer	Nutzung
CSP	8800	beliebige CSTA-Anwendung
CMD	8900	reserviert für TAPI 120 Clients; unabhängig von der Anzahl der Clients wird genau ein logischer CSTA-Link belegt

Externe CSTA-Anwendungen bzw. TAPI 120 Service Provider müssen die IP-Adresse des UC Servers bzw. des Systems mit der entsprechenden Portnummer verwenden um die Verbindung herzustellen. Die entsprechende IP-Adresse wird im WBM unter Applikationsauswahl angezeigt.

CSTA-Links

Standardmäßig steht ein CSTA-Link des CSP Port für externe CSTA-Anwendungen zur Verfügung. Drei weitere CSTA-Links sind standardmäßig folgenden integrierten CSTA-Anwendungen bzw. Diensten zugeordnet:

- CMD (CSTA Message Dispatcher) für TAPI 120 Clients am CMD Port
- DSS (Direct Station Server)
- UC Suite

Falls diese CSTA-Anwendungen bzw. Dienste nicht benötigt werden, können bei Bedarf die entsprechenden CSTA-Links externen CSTA-Anwendungen zugeordnet werden.

Plus-Produkte

Folgende Flags sind im System stets aktiviert:

- Vorwahl stets mit Rufnummer übertragen
- erweitertes CSTA-CAUSE Handling
- CSTA CSP Signalisierung
- MULAP Monitoring

Verwandte Themen

- Unterstützte Telefone

22.1.1 Wie Sie die Portnummer für CSTA ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **Grundeinstellungen > Port-Verwaltung**.

4) Geben Sie in der Zeile für **CSP** im Eingabefeld der Spalte **Port-Nummer** die gewünschte Portnummer ein.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

6) Führen Sie einen Neustart des Systems durch.

Verwandte Themen

- OpenScape Business TAPI 120

22.1.2 Wie Sie den CMD für die Nutzung von TAPI 120 aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Middleware**.

3) Klicken Sie im Menübaum auf **Middleware > CSTA Message Dispatcher (CMD)**.

4) Klicken Sie auf die Registerkarte **Einstellungen - CSTA Message Dispatcher (CMD)**.

5) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie den CMD aktivieren möchten, aktivieren Sie in Bereich **Aktivierung** das Kontrollkästchen **Dienst wird automatisch gestartet**.
- Wenn Sie den CMD deaktivieren möchten, deaktivieren Sie in Bereich **Aktivierung** das Kontrollkästchen **Dienst wird automatisch gestartet**.

6) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie Auto Registration für Clients nutzen möchten, aktivieren Sie in Bereich **Autom Registrierung** das Kontrollkästchen **Autom. Registrierung des Clients aktiviert**.
- Wenn Sie Auto Registration für Clients nicht nutzen möchten, deaktivieren Sie in Bereich **Autom Registrierung** das Kontrollkästchen **Autom. Registrierung des Clients aktiviert**.

7) Klicken Sie auf **Übernehmen**.

Verwandte Themen

- OpenScape Business TAPI 120

22.1.3 Wie Sie den DSS-Server für die Nutzung von netzweiten DSS-Tasten aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Middleware**.

3) Klicken Sie im Menübaum auf **Middleware > DSS-Server**.

4) Klicken Sie auf die Registerkarte **Einstellungen - DSS-Server**.

5) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie den DSS-Server aktivieren möchten, aktivieren Sie in Bereich **Aktivierung** das Kontrollkästchen **Der Dienst wird automatisch gestartet**.
- Wenn Sie den DSS-Server deaktivieren möchten, deaktivieren Sie in Bereich **Aktivierung** das Kontrollkästchen **Der Dienst wird automatisch gestartet**.

6) Klicken Sie auf **Übernehmen**.

22.1.4 Wie Sie den CSP aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Middleware**.

3) Klicken Sie im Menübaum auf **Middleware > CSTA Service Provider (CSP)**.

4) Klicken Sie auf die Registerkarte **Einstellungen - CSTA Service Provider (CSP)**.

5) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie den CSP aktivieren möchten, aktivieren Sie in Bereich **Aktivierung** das Kontrollkästchen **Dienst wird automatisch gestartet**. Geben Sie auch eine CSTA-Benutzer-ID und ein CSTA-Benutzer-Passwort ein, damit eine Applikation CSTA nutzen kann.
- Wenn Sie den CSP deaktivieren möchten, deaktivieren Sie in Bereich **Aktivierung** das Kontrollkästchen **Dienst wird automatisch gestartet**.

INFO: Wenn CSP deaktiviert wird, kann TAPI 120 (über CMD), TAPI 170, DSS-Server und UC Suite nicht betrieben werden!

---

6) Klicken Sie auf **Übernehmen**.

22.1.5 Wie Sie Media Extension Bridge aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Middleware**.

3) Klicken Sie im Menübaum auf **Middleware > Media Extension Bridge (MEB)**.

4) Klicken Sie auf die Registerkarte **Einstellungen - Media Extension Bridge (MEB)**.

5) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie Media Extension Bridge nutzen möchten, aktivieren Sie in Bereich **Aktivierung** das Kontrollkästchen **Dienst wird automatisch gestartet**.
- Wenn Sie diesen CSTA-Link freigeben möchten, deaktivieren Sie in Bereich **Aktivierung** das Kontrollkästchen **Dienst wird automatisch gestartet**.

6) Klicken Sie auf **Übernehmen**.

22.2 OpenScape Business TAPI 120/170

OpenScape Business TAPI 120 und OpenScape Business TAPI 170 sind neben CallBridge Collection zwei für die Systemarchitektur und Netzwerktopologie von OpenScape Business optimierte TAPI Service Provider (TSP), die TAPI-basierten Applikationen die Microsoft TAPI Schnittstelle für die Anbindung an das OpenScape Business Kommunikationssystem zur Verfügung stellen.

Die Anschaltung an OpenScape Business erfolgt ausschließlich über LAN. Hardware- und Software-Zusatzkomponenten, wie CSTA Message Dispatcher (CMD) oder CSTA Service Provider (CSP), werden zum Betrieb an OpenScape Business nicht mehr benötigt. Die Lizenzierung ist teilnehmer-bezogen und unterscheidet nicht zwischen OpenScape Business TAPI 120 oder TAPI 170 Teilnehmer. Die Lizenzierungspflicht beginnt mit dem ersten TAPI-Teilnehmer.

Die Wahl des geeigneten TAPI Services Providers hängt im wesenlichen von der Anzahl der anzuschaltenden Client PC mit TAPI-Applikationen und der vorhandenen IT-Infrastruktur sowie den verwendeten Telefonen ab.

- **CallBridge Collection**
  wird als klassischer First Party TAPI Serviceprovider an Systemtelefonen, die eine LAN- oder USB-Schnittstelle besitzen, eingesetzt. Sie eignet sich für Installationen mit nur wenigen PCs. Ein LAN ist für den Betrieb der CallBridge Collection nicht erforderlich. Die CallBridge Collection wird auf jedem PC installiert, auf dem eine TAPI-Applikation betrieben wird. Analoge, Cordless- sowie Systemtelefone ohne USB-/IP-Schnittstelle werden nicht unterstützt. TAPI-Anschaltungen über die CallBridge Collection ist nicht lizenziert.
- **OpenScape Business TAPI 120**
  wird vorzugsweise als First Party TAPI Serviceprovider in Microsoft-Netzwerken mit oder ohne Domain Controller eingesetzt, wenn auch analoge, Cordless- oder Systemtelefone ohne USB-/IP-Schnittstelle in Verbindung mit

der TAPI-Applikation betrieben werden sollen. Der TAPI 120 Service Provider wird auf jedem PC Client installiert, auf dem eine TAPI-Applikation betrieben wird.
TAPI-Anschaltungen über OpenScape Business TAPI 120 unterliegen der Lizenzierung innerhalb von OpenScape Business. Zur Anschaltung an OpenScape Business wird abhängig von der Betriebs-/Anschaltungsart entweder ein CSTA Link oder ein Link zum WebServices Interface benötigt - unabhängig davon, wie viele TAPI 120 Clients betrieben werden. Der TAPI-seitige Leistungsumfang hängt von der Betriebs-/Anschaltungsart ab.

- **OpenScape Business TAPI 170**
  ist ein klassischer "Third Party" TAPI Service Provider. Er wird auf einem Server im LAN installiert und zentral an das OpenScape Business System angeschaltet. TAPI 170 kann alternativ zum TAPI 120 eingesetzt werden, wenn ein Domain Controller im Microsoft-Netzwerk vorhanden ist. Bei der Nutzung der sogenannten Remote TAPI Funktion entfällt die Installation des TAPI Service Providers auf den Client PCs. Diese bietet bei Installationen mit vielen Client PCs deutliche Zeitvorteile. In den nachfolgenden Konstellationen ist OpenScape Business TAPI 170 jedoch zwingend zu verwenden.
  - Anbindung von TAPI-Teilnehmern an vernetzte OpenScape Business Systeme, wenn die TAPI-Teilnehmer in verschiedenen Knoten lokalisiert sind.
  - Anbindung von TAPI-Applikationen, die auf einem Terminalserver betrieben werden.
  - Anbindung von serverbasierenden TAPI-Applikationen.

  TAPI-Anschaltungen über OpenScape Business TAPI 170 unterliegt der Lizenzierung innerhalb von OpenScape Business. Zur Anschaltung an OpenScape Business wird ein CSTA Link benötigt - unabhängig davon, wie viele TAPI 170 Teilnehmer betrieben werden.

22.2.1 OpenScape Business TAPI 120

OpenScape Business TAPI 120 ist ein 1st Party Telephony Service Provider, der den Microsoft TAPI V2.1 Funktionsumfang unterstützt. OpenScape Business TAPI 120 ermöglicht Windows-basierten CTI-Applikationen ein an OpenScape Business angeschaltetes Systemtelefon zu monitoren und zu steuern.

OpenScape Business TAPI 120 kann alternativ über die CSTA-Schnittstelle (CSTA Modus) oder über das WebServices Interface WSI (UC Smart Modus) an OpenScape Business angeschaltet werden. Ein Mischbetrieb in der Anschaltung an einem System ist nicht möglich. Ist im OpenScape Business System eine UC Booster Card gesteckt oder ist ein UC Booster Server angeschaltet, kann TAPI 120 nur im CSTA Modus betrieben werden. Die Systemvoraussetzungen, die maximale Anzahl der TAPI-Teilnehmer und der TAPI-seitige Leistungsumfang hängt von den Betriebmodi ab.

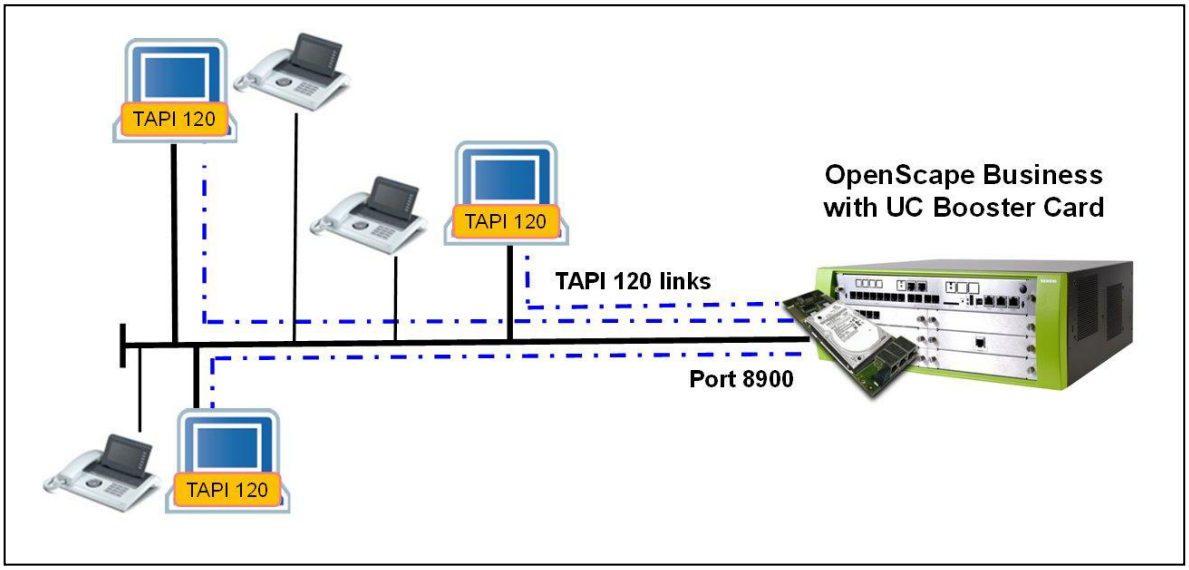
OpenScape Business TAPI 120 Anschaltungen

Die OpenScape Business TAPI 120 Software wird auf einem Microsoft Windows Client PC installiert. Die Verbindung zum OpenScape Business System erfolgt

über LAN. Eine physikalische Verbindung zwischen dem Windows PC und dem Telefon ist nicht erforderlich.

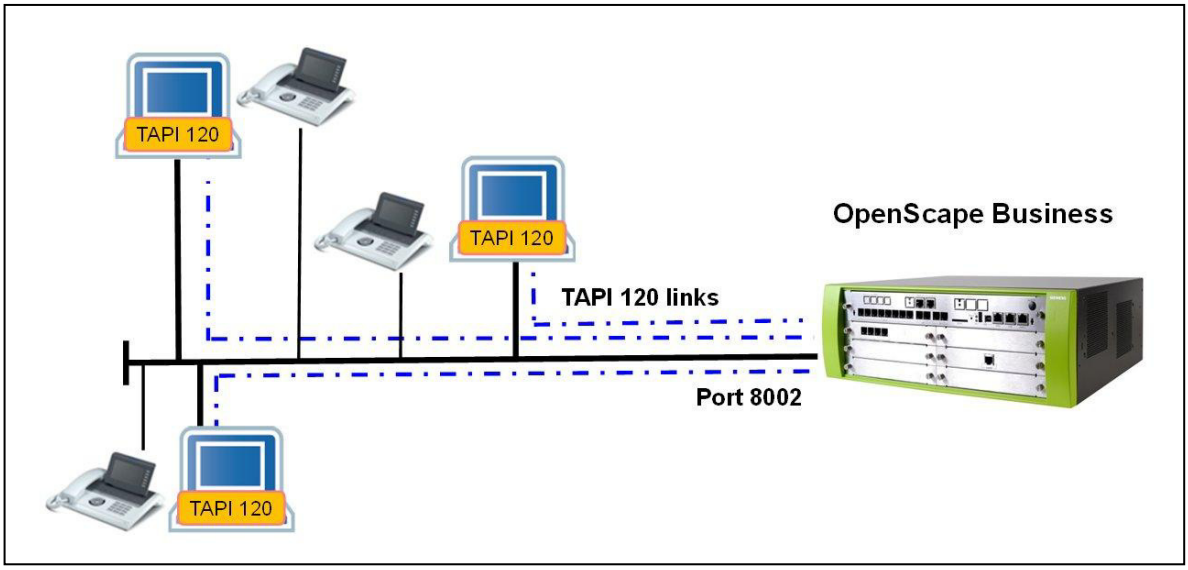
- **TAPI 120 CSTA Modus**
  Alle TAPI 120 Client PCs werden an denselben CSTA Link von OpenScape Business angeschaltet. OpenScape Business multiplext intern alle TAPI 120 Verbindungen.
  TAPI 120 im CSTA Modus unterstützt OpenScape Business X3/X5/X8 und OpenScape Business S.

  Bild: TAPI 120 im CSTA Modus mit OpenScape Business X5R und UC Booster Card



- **TAPI 120 UC Smart Modus**
  Alle TAPI 120 Client PCs werden über LAN und WebServer Interface an das Mainboard von OpenScape Business angeschaltet. OpenScape Business multiplext intern alle TAPI 120 Verbindungen.
  TAPI 120 im CSTA Modus unterstützt OpenScape Business X1/X3/X5/X8.

Bild: TAPI 120 im UC Smart Modus mit OpenScape Business X5R



Leistungsmerkmale

Folgende Leistungsmerkmale werden unterstützt:

Leistungsmerkmal	TAPI 120 CSTA	TAPI 120 UC Smart
Zentral über LAN angeschalteter First-Party TAPI Service Provider	X	X
Kompatibel mit dem Microsoft TAPI 2.1 Standard	X	X
Anschaltung an OpenScape Business Einzelsystemen	X	X
Unterstützung der OpenScape Business CTI Firewall	X	-
Über TAPI unterstützte Funktionen		
Rufsignalisierung kommender und gehender Gespräche mit Identifikation der Rufnummern und der Herkunft des Gespräches	X	X
Zusatzinformationen in der Rufsignalisierung bei umgeleiteten Gesprächen	X	X
Gesprächsannahme interner und externer Anrufe	X	X
gesteuerter Verbindungsaufbau zu internen und externen Gesprächspartnern	X	X
manuelle Wahl / DTMF Nachwahl	X	X
Auslösung bestehender Gespräche	X	X
Aufbau eines Rückfragegespräches zu internen und externen Gesprächspartnern	X	X
Makeln	X	X
begleitete Anrufübergabe	X	X

Leistungsmerkmal	TAPI 120 CSTA	TAPI 120 UC Smart
begleitete Anrufübergabe mit nachfolgender Wahl des Rückfrageziels (One-Step Transfer)	X	X
unbegleitete Anrufübergabe (Blind-Transfer)	X	-
Anrufumleitung setzen und löschen	X	X
Anrufschutz setzen und löschen	X	X
Konferenz einleiten	X	-
Konferenz erweitern	X	-
kommenden Ruf weiterleiten	X	-
Gezielte Übernahme (Call Pickup)	X	-
Gruppenrufsignalisierung und Übernahme Gruppenruf (Group Pickup)	X	-
Parken von bestehenden Gesprächen	X	-
Wiederaufnahme geparkter Gespräche	X	-
manuelles Halten von bestehenden Gesprächen	X	-
Wiederaufnahme manuell gehaltener Gespräche	X	-
Rückruf setzen	X	-
Unterstützung von Code-gesteuerten Funktionen	X	-
gesprächsbezogener Datenaustausch zwischen TAPI-Applikationen	X	-
Steuerung der Tasten bei Systemtelefonen (HFA)	X	-
Steuerung der Mikrofon-Verstärkung bei Systemtelefonen (HFA)	X	-
Steuerung/Auswahl der Nutzung von Handset/Lautsprechen/Headset bei Systemtelefonen (HFA)	X	-
Steuerung der Lautstärke von Handset/Lautsprecher/Headset Tastatur bei Systemtelefonen (HFA)	X	-
Zugriff auf optiPoint / OpenStage Displays und den LEDs (mit Limitierung auf 50 aktive Displays pro System)	X	-

Maximalwerte

Die maximal Anzahl von TAPI 120 Client PCs, die an OpenScape Business angeschaltet werden können ist modellabhängig (siehe *Vertriebliche Ausbaustufen*).

Freigegebene Betriebssysteme

Die aktuell freigegebenen Betriebssysteme für den Microsoft Windows Server, den Terminal-Server und den Remote Client PC sind in der aktellen Vertriebsinformation aufgelistet.

Es können nur Microsoft Windows Betriebssysteme in Verbindung mit TAPI 120 verwendet werden.

Bei Installationen auf Terminal-Servern ist OpenScape Business TAPI 170 anstelle von OpenScape Business TAPI 120 einzusetzen.

Lizenzierung

Die Verwendung von OpenScape Business TAPI 120 ist auf Teilnehmerbasis lizenziert. Die TAPI-Lizenzen werden innerhalb des OpenScape Business Systems verwaltet und sind für beide Betriebsarten des TAPI 120 einsetzbar. Bei Verwendung des Leistungsmerkmals MULAP ist für jeden Teilnehmer innerhalb der MULAP eine TAPI-Lizenz erforderlich.

INFO: Bei TAPI 120 im UC Smart Modus sind keine UC Smart Lizenzen erforderlich.

Software-Bereitstellung

Die OpenScape Business TAPI 120 Software wird auf einem eigenen Datenträger ausgeliefert. Sie ist nicht Bestandteil der OpenScape Business System Software.

Hardware-Anforderungen

Der PC muss mindestens den von Microsoft vorgegebenen Systemanforderungen für das eingesetzte Betriebssystem sowie den Anforderungen der TAPI-Applikation entsprechen. Zusätzlich wird ein Ethernet LAN Interface benötigt.

- bei TAPI 120 CSTA
  Unabhängig von der Anzahl angeschalteter TAPI 120 Clients wird ein CSTA Link von OpenScape Business benötigt. Hierfür ist ein OpenScape Business UC Booster (Card oder Server) Voraussetzung.
- bei TAPI 120 UC Smart
  Es wird das WebServices Interface benötigt. Es darf kein OpenScape Business UC Booster (Card oder Server) im/am System vorhanden sein.

Unterstützte Endgeräte

Die unterstützten Endgeräte wie auch die unterstützten Leistungsmerkmale an diesen Endgeräten hängen vom CSTA- bzw vom WSI-Funktionsumfang des eingesetzten OpenScape Business Systems ab. Diese Informationen sind in der OpenScape Business Vertriebsinformation enthalten.

Standardmäßig von TAPI 120 belegter IP-Port/IP-Adresse

In der Betriebsart TAPI 120 CSTA belegt der CSTA Link zur OpenScape Business den IP-Port 8900.

In der Betriebsart TAPI 120 UC Smart belegt der WSI-Link zur OpenScape Business den IP-Port 8802 für eine verschlüsselte Verbindung (HTTPS) oder 8801 für eine unverschlüsselte Verbindung (HTTP).

In der TAPI 120 Konfiguration muss die IP-Adresse des OpenScape Business Systems entsprechend der Betriebsart eingeben werden. Diese IP-Adresse wird im WBM unter **Applikationsauswahl** angezeigt.

Verwandte Themen

- Wie Sie die Portnummer für CSTA ändern
- Wie Sie den CMD für die Nutzung von TAPI 120 aktivieren oder deaktivieren

22.2.2 OpenScape Business TAPI 170

OpenScape Business TAPI 170 ist ein 3rd Party Telephony Service Provider, der den Microsoft TAPI V2.1 Funktionsumfang unterstützt. TAPI 170 ermöglicht Microsoft Windows basierenden CTI-Applikationen mehrere an OpenScape Business angeschaltete Telefone gleichzeitig zu monitoren und zu steuern.

Leistungsmerkmale

OpenScape Business TAPI 170 bietet folgende Leistungsmerkmale:

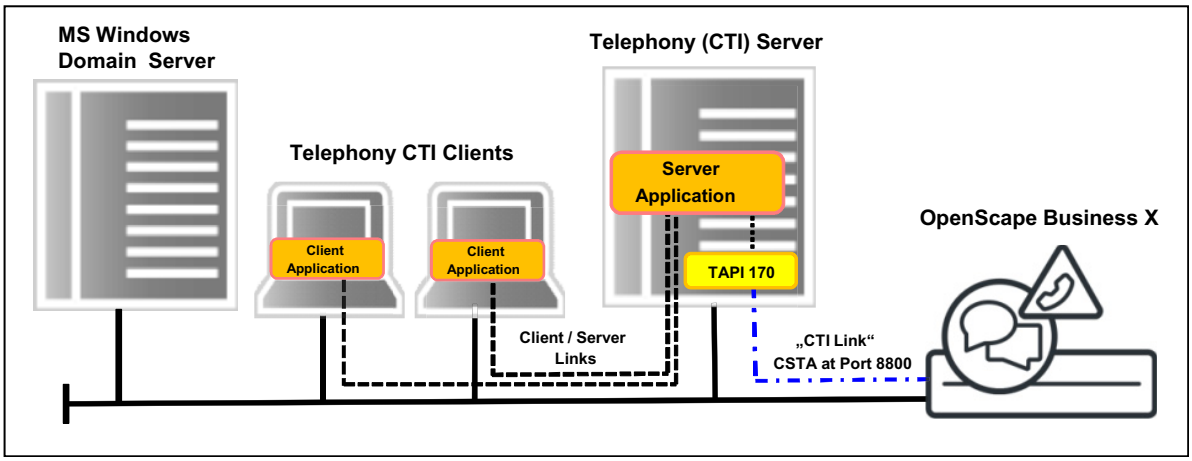
- zentral angeschalteter 3rd Party TAPI Service Provider
- kompatibel mit dem Microsoft TAPI 2.1 Standard
- Telefonie-Funktionen sind auf jedem angeschalteten PC Client über die TAPI 2.1 Client/Server Architektur verfügbar
- keine zusätzliche TSP Client Software erforderlich
- Unterstützte Telefoniefunktionen:
  - Kommende/gehende Wahl vom PC
  - Übertragung der kommenden Rufnummer, sofern signalisiert
  - Rückfrage und Transfer
  - Makeln
  - Konferenz
  - Anrufumleitung
  - Anrufer weiterleiten
  - Annehmen eines Anrufs durch die Applikation
  - Auslösen eines Anrufs durch die Applikation
  - Übergabe vor/nach Melden
  - Übertragung von Leistungsmerkmalcodes
  - Monitoring des Telefons (Rufzustände, Ausfall, etc.)
  - Bereitstellung eines ACD-Interfaces
  - Monitoring/Zugriff auf Tastatur bei Systemtelefonen (HFA)
  - Ansteuerung von Display/LED bei Systemtelefonen (HFA)
  - Anschaltung an OpenScape Business Einzelsysteme sowie vernetzte Systeme
  - Unterstützung von MULAP-Teilnehmern/-Rufnummern

OpenScape Business TAPI 170 Anschaltungen

Die OpenScape Business TAPI 170 Software wird auf einem Microsoft Windows Server im Netzwerk installiert. Die Anbindung an OpenScape Business erfolgt über einen CSTA Link. Eine physikalische Verbindung zwischen dem Windows PC und dem Telefon ist nicht erforderlich. OpenScape Business TAPI 170 kann in unterschiedlichen Betriebsarten an Einzelsystemen oder im OpenScape Business Netzwerk eingerichtet werden. TAPI Server und Clients müssen vom gleichen Netzwerk Domain Controller verwaltet werden.

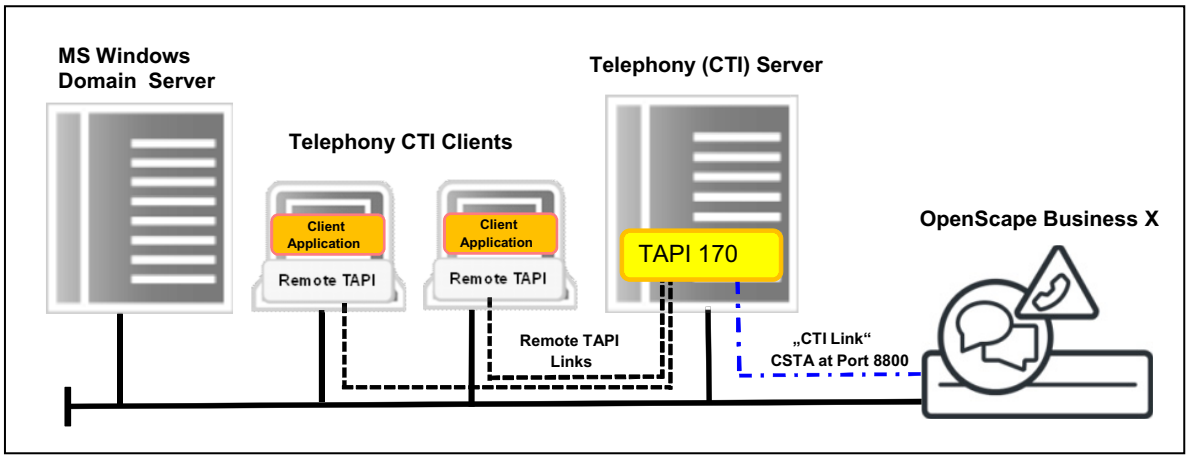
- **Anschaltung serverbasierter TAPI Applikationen an OpenScape Business über TAPI 170**
  Die Server-Applikation und die TAPI 170 Software werden auf dem sogenannten "Telefonie-Server" im Netzwerk installiert. Die Server-Applikation stellt ihren zugehörigen Clients im Netzwerk die Telefoniefunktionen für die Teilnehmer zur Verfügung, die innerhalb von OpenScape Business TAPI 170 konfiguriert sind. Die TAPI 170 Software wird über LAN an die CSTA Schnittstelle von OpenScape Business angebunden. Für diese Anschaltung wird ein CSTA Link von OpenScape Business sowie je eine TAPI-Lizenz für jeden eingerichteten TAPI-Teilnehmer benötigt.

  Bild: Serverbasierte TAPI-Applikation über TAPI 170 an OpenScape Business



- **Anschaltung clientbasierter TAPI-Applikationen an OpenScape Business über TAPI 170 mit "Remote TAPI" Funktion**
  In diesem Szenario wird die OpenScape Business TAPI 170 Software auf einem Server im Netzwerk installiert. Auf den Client PCs mit den TAPI-Applikationen wird sogenannte "Remote TAPI" Funktion freigeschaltet, über die die TAPI-Applikation auf dem Client mit der TAPI 170 Software auf dem Server kommuniziert. Auf den Client muss hierzu keine TAPI 170 Software installiert werden. Die TAPI 170 Software wird über LAN an die CSTA Schnittstelle von OpenScape Business angebunden. Für diese Anschaltung wird ein CSTA Link von OpenScape Business sowie je eine TAPI Lizenz für jeden eingerichteten TAPI Teilnehmer benötigt.

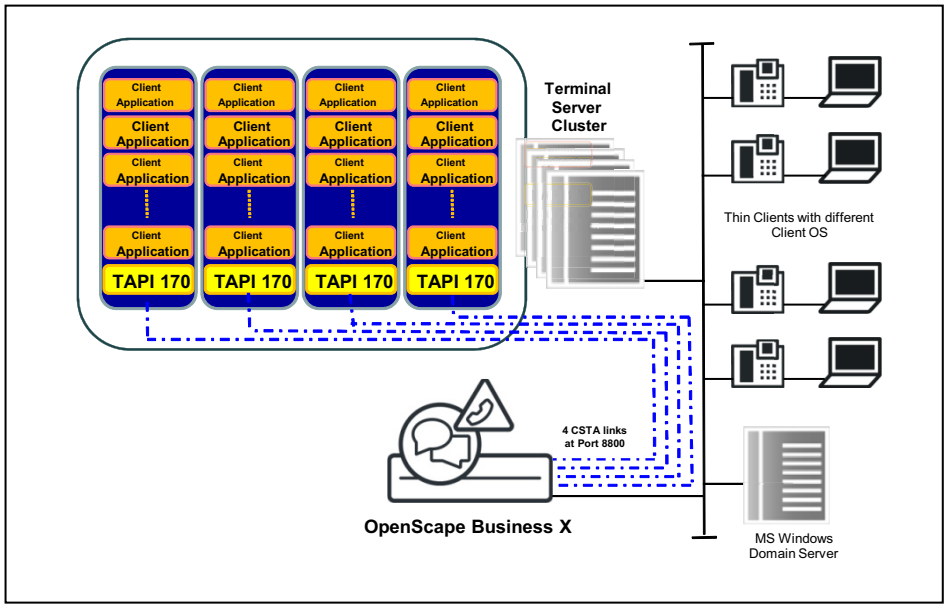
Bild: Clientbasierte TAPI-Applikation über "Remote TAPI" an OpenScape Business



- **Anschaltung Terminal-Server basierter TAPI-Applikationen an OpenScape Business über TAPI 170**
  In diesem Szenario sind die Client basierten TAPI-Applikationen auf einem oder mehreren Terminal-Servern installiert. Die TAPI 170 Software wird in diesen Fall mit auf dem Terminal-Server installiert. Im Fall eines aus mehreren Terminal-Servern bestehenden Clusters muss die TAPI 170 Software auf jedem Terminal-Server im Cluster installiert werden. Jede installierte TAPI 170 Software wird über LAN an OpenScape Business angebunden. Für jede auf einem Terminal-Server installierte TAPI 170 Software wird ein CSTA Link von OpenScape Business benötigt. Weiterhin ist eine TAPI Lizenz für jeden eingerichteten TAPI Teilnehmer erforderlich.
  Die maximal mögliche Anzahl von OpenScape Business TAPI 170 Servern in Verbindung mit OpenScape Business darf nicht überschritten werden.

  INFO: Es können nur so viele Terminal-Server im Cluster bedient werden wie freie CSTA Links innerhalb von OpenScape Business zur Anschaltung der TAPI 170 Software zur Verfügung stehen. Der Maximalwert der möglichen Anschaltungen verringert sich, wenn die CSTA Links von OpenScape Business durch andere CSTA Applikationen belegt sind.

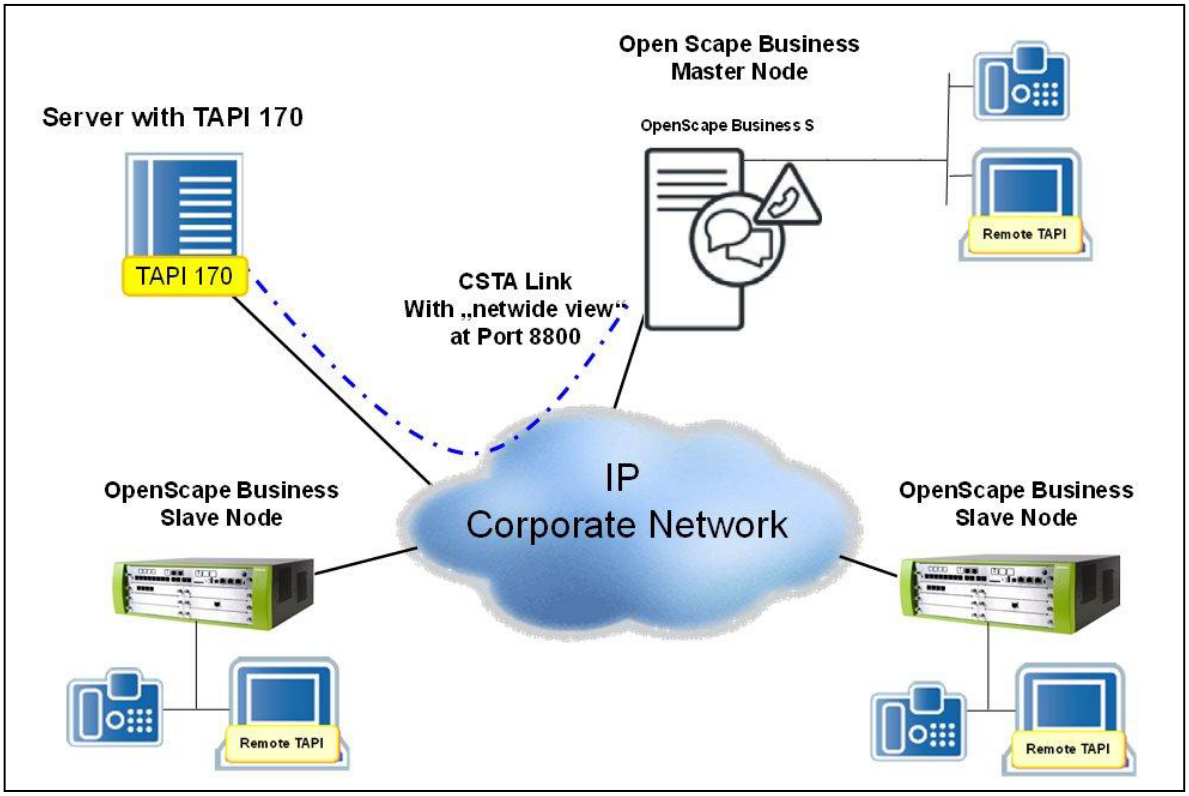
Bild: Client basierte TAPI Applikation auf Terminal-Server an OpenScape Business



- **Anschaltung von TAPI 170 an vernetzte OpenScape Business Systeme**
  Bei vernetzten OpenScape Business Systemen wird die TAPI 170 Software auf einem Server installiert, der über LAN an die CSTA Schnittstelle des Master-Knotens angeschaltet wird. Diese Anschaltung ist unabhängig von den zuvor erwähnten Betriebsarten des TAPI 170 Service Providers (Remote TAPI oder serverbasierte Anschaltung). Für die Realisierung wird ein CSTA Link von OpenScape Business Master-Konten sowie je eine TAPI Lizenz für jeden TAPI Teilnehmer im Netzwerk benötigt.

  INFO: Über den Master-Knoten erhält der TAPI 170 den netzweiten Zugriff auf alle Teilnehmer im Netzwerk. Bei einer Anschaltung des TAPI 170 an einem Slave-Knoten anstatt am Master-Knoten kann TAPI 170 nur auf die Teilnehmer des Slave-Knotens zugreifen. Bei Einsatz von mehreren TAPI 170 in einem Terminal-Server Cluster ist für jeden TAPI 170 ein CSTA Link zum Master Knoten erforderlich.

Bild: Anschaltung von TAPI 170 an vernetzte OpenScape Business Systeme



Ausbaugrenzen

Die maximal Anzahl von TAPI 170 Client PCs, die an OpenScape Business angeschaltet werden können ist modellabhängig. Weitere Informationen hierzu sind im Kapitel 1.3.9.4 enthalten

Freigegebene Betriebssysteme

Die aktuell freigegebenen Betriebssysteme für den Microsoft Windows Server, den Terminal-Server und den Remote Client PC sind in der aktellen Vertriebsinformation aufgelistet.

Es können nur Microsoft Windows Betriebssysteme in Verbindung mit TAPI 170 verwendet werden.

Das Lizenzmodell von Microsoft erfordert neben der Lizenz für das Server Betriebssystem, auch entsprechende Microsoft Device oder User CALs in der für den geplanten Ausbau benötigten Anzahl. Diese CALs sind nicht Bestandteil der Lieferung von OpenScape Business TAPI 170 und müssen immer separat beschafft werden. Unter bestimmten, von Microsoft vorgegebenen Bedingungen, kann für OpenScape Business TAPI 170 auch ein "Windows Server for embedded systems" mit der sogenannten "Embedded Telco Lizenz" verwendet werden.

Lizenzierung

Die Verwendung von OpenScape Business TAPI 170 ist auf Teilnehmerbasis lizenziert. Die Lizenzen werden innerhalb des OpenScape Business Systems verwaltet. Bei Verwendung des Leistungsmerkmals MULAP ist für jeden Teilnehmer innerhalb der MULAP eine TAPI Lizenz erforderlich.

Software-Bereitstellung

Die OpenScape Business TAPI 170 Software wird auf einem eigenen Datenträger ausgeliefert. Sie ist nicht Bestandteil der OpenScape Business System Software.

Hardware-Anforderungen

Für die Anschaltung von OpenScape Business TAPI 170 wird unabhängig von der Anzahl angeschalteter TAPI 170 Clients ein CSTA Link von OpenScape Office benötigt. Dies gilt auch für vernetzte OpenScape Business Systeme.

Der PC muss mindestens den von Microsoft vorgegeben Systemanforderungen für das eingesetzte Betriebssystem entsprechen, vorausgesetzt dass keine weiteren SW-Applikationen außer TAPI 170 betrieben werden. Zusätzlich wird ein Ethernet LAN Interface benötigt.

Unterstützte Endgeräte

Die unterstützten Endgeräte wie auch die unterstützten Leistungsmerkmale an diesen Endgeräten hängen vom CSTA- bzw vom WSI-Funktionsumfang des eingesetzten OpenScape Business Systems ab. Diese Informationen sind in der OpenScape Business Vertriebsinformation enthalten.

22.3 Web Services Interface

Das integrierte Web Services Interface ermöglicht das Monitoring und die Steuerung von Telefonie-Ressourcen in einem System mit UC-Benutzern.

Leistungsmerkmale

Das Web Services Interface bietet folgende Leistungsmerkmale:

- Zugriff via Ethernet LAN (TCP/IP)
- Unterstützung von HTTP und HTTPS
- Unterstützung für einzelne Systeme
- benutzerorientierte, klar strukturierte Funktionen für:
  - Steuerung von Anrufen
  - Steuerung von Geräten
  - Monitoring von Geräten
  - Telefonbücher
  - Journal der Teilnehmer
  - Anwesenheitsstatus der Teilnehmer

WebServer WebSessions

Die Anzahl der verfügbaren Web Server Sessions gilt für alle entsprechenden Anwendungen gemeinsam, wie z. B. myPortal for Mobile, Application Launcher, OptiClient Attendant (Server) und OptiClient BLF.

Interne Monitorpunkte

Die internen Monitorpunkte sind unabhängig von den Monitorpunkten der CSTA-Schnittstelle. Falls mehrere Anwendungen denselben UC-Benutzer über das Web Services Interface überwachen, verwendet der Webserver dafür nur einen einzigen internen Monitorpunkt.

Ports

Folgende Portnummern stehen zur Verfügung:

Port	Protokoll
8801	HTTP (unverschlüsselt)
8802	HTTPS (verschlüsselt)

22.4 Open Directory Service

Open Directory Service ist ein offener, integrierter Metaverzeichnisdienst auf den unterschiedlichste Arten von Clients, Anwendungen und Kommunikationsgeräten eines Unternehmens zugreifen können. Open Directory Service ermöglicht einerseits die zusätzliche Einbindung von Kontaktdaten externer Datenbanken in Verzeichnisse des Systems und andererseits die Bereitstellung von Verzeichnissen an Clients, Kommunikationsgeräte und Anwendungen.

Open Directory Service läuft auf der Basis von OpenLDAP als eigener Dienst. Firewalls müssen für Port 389 geöffnet sein. Open Directory Service ist standardmäßig deaktiviert.

Interne Datenquellen

Folgende Datenquellen stehen in Open Directory Service standardmäßig zur Verfügung:

- OpenScape ...: diese beinhaltet
  - internes Verzeichnis
  - externes Verzeichnis
- zentrale Kurzwahlnummern

Für diese Datenquellen sind die Feldnamen dem Datenschema von Open Directory Service fest zugeordnet.

Diese Datenquellen können nicht gelöscht oder geändert werden.

Externe Datenquellen

Als Administrator können Sie Kontaktdaten aus folgenden Arten von Datenbanken als Datenquellen für lesenden Zugriff via ODBC einbinden:

- Microsoft SQL Server
- PostgreSQL
- Sybase SQL Server

Maximale Anzahl unterschiedlicher Arten von Datenbanken: 3

Maximale Anzahl externer Datenquellen: 4

Sorgen Sie dafür, dass Open Directory Service berechtigt ist, auf die externe Datenbank zuzugreifen. Kontaktieren Sie hierfür vorab den zuständigen Datenbankadministrator. Unter Umständen muss in der externen Datenbank für den Zugriff durch das System ein eigener Benutzer hinzugefügt werden.

Externe Datenquellen können sowohl im Rahmen der Verzeichnissuche als auch bei der Auflösung von Rufnummern in Namen genutzt werden.

Sie können direkten Zugriff auf eine Datenbanktabelle einer externen Datenquelle konfigurieren oder eine benutzerdefinierte SQL-Abfrage für die Datenquelle.

Eine Spalte, die als ID dient, muss eindeutige Werte enthalten. Verwenden Sie die Eigenschaft UNIQUE oder PRIMARY KEY um dies zu gewährleisten.

Bei der Einbindung externer Datenbanken gelten folgende Einschränkungen:

- Die Sonderzeichen ´[]'" werden vom ODS in Tabellennamen und Spaltennamen nicht unterstützt.
- Die Spaltentypen "nchar" und "nvarchar" werden vom ODS nicht unterstützt.

Benutzerdefinierte SQL-Abfragen für externe Datenquellen

Benutzerdefinierte SQL-Abfragen unterstützen auch verknüpfte Tabellen, z. B.:

```
SELECT * FROM users LEFT OUTER JOIN phonenumbers ON users.id
= phonenumbers.uid;
```

Die Datenstruktur muss von der Art 1:1 oder n:1 sein, d. h. jeder Datensatz darf nur eine einzige Zeile haben.

Der Zugriff mittels benutzerdefinierter SQL-Abfragen kann unter Umständen deutlich langsamer ablaufen als bei direktem Zugriff auf eine Datenbanktabelle.

Benutzerdefinierte SQL-Abfragen mit potentiellen Sicherheitsrisken werden nicht ausgeführt, z. B. zum:

- Ändern von Daten
- Anhalten des SQL-Servers
- Ausführen von Programmen durch den SQL-Server
- Ändern von Benutzerrechten

Benutzerdefinierte SQL-Abfragen mit folgenden SQL-Kommandos werden deshalb nicht ausgeführt:

- `CHECKPOINT`
- `CLOSE`

- CLUSTER
- COMMIT
- COPY
- CREATE
- DEALLOCTAE
- DECLARE
- DELETE
- DISCARD
- DO
- DROP
- END
- EXECUTE
- EXPLAIN
- FETCH
- GRANT
- INSERT
- LOAD
- LOCK
- MOVE
- PREPARE
- REASSIGN OWNED
- REINDEX
- RELEASE SAVEPOINT
- RESET
- REVOKE
- SAVEPOINT
- SECURITY LABEL
- SELECT INTO
- SET
- SHOW
- START TRANSACTION
- TRUNCATE
- UNLISTEN
- UPDATE
- VACUUM
- VALUES

Feldzuordnung für Datenquellen

Für diese Datenquellen können Sie die Zuordnung der Feldnamen zum Datenschema von Open Directory Service anpassen. Sie können jedem Feld im Datenschema von Open Directory Service höchstens ein Feld der externen

Datenquelle zuordnen. Sie können ein Feld der externen Datenquelle mehreren Feldern im Datenschema von Open Directory Service zuordnen.

LDAP-Ausgabezuordnungen

Eine LDAP-Ausgabezuordnung legt fest, welche der Felder des Datenschemas von Open Directory Service via LDAP ausgegeben werden sollen, z. B. für spezifische LDAP-Clients oder für verschiedene Gruppen von Teilnehmern, welche nicht alle Details sehen sollen, sondern nur eine definierte Untermenge.

Die LDAP-Ausgabezuordnung **web** steht standardmäßig zur Verfügung und kann nicht gelöscht oder geändert werden. In ihr sind alle Felder des Datenschemas von Open Directory Service der LDAP-Ausgabe fest zugeordnet. Sie können weitere LDAP-Ausgabezuordnungen konfigurieren.

Über den Parameter dc im LDAP-Login können LDAP-Clients auf eine bestimmte LDAP-Ausgabezuordnung zugreifen, z. B.: `dc=web`.

Normalisierung von Rufnummern in das kanonische Format

Für jede Datenquelle können Sie die Normalisierung von Rufnummern in das kanonische Format konfigurieren. Dabei werden Leerzeichen, Klammern, Bindestriche und Kommata entfernt. Dies ist für die korrekte Identifizierung von Anrufernamen sowie für die Desktop-Wahl erforderlich. Auf die Normalisierung sollten Sie nur verzichten, wenn die Rufnummern in der verwendeten Datenquelle bereits im kanonischen Format vorliegen. Sie können für die Normalisierung relevante Werte wie Ortsnetzkennzahl etc. aus dem System automatisch eintragen lassen. Falls sich die externe Datenbank an einem anderen Standort befindet als das System, müssen Sie diese Werte eventuell anpassen.

Status der Datenquellen

Die Statusanzeige unter **OpenDirectory > Datenquellen** hat folgende Bedeutung:

Farbe	Status
grün	aktiv
rot	ODBC und LDAP nicht ok, Konfiguration fehlerhaft oder Datenquelle nicht verfügbar
gelb	LDAP nicht ok: Open Directory Service neu starten
grau	Konfiguration unvollständig

Bereitstellung von Verzeichnissen

Folgende Arten von Clients, Kommunikationsgeräten und Anwendungen können die von Open Directory Service bereitgestellten Verzeichnisse nutzen:

- UC Clients
- Application Launcher
- Systemtelefonbuch
- OpenStage Telefone mit lokaler LDAP-Unterstützung
- DECT-IP-Telefone (via LDAP)

- SIP-Telefone (via LDAP)
- Anwendungen, z. B. CRM Suites wie Microsoft Dynamics CRM (via LDAP, ODBC oder OpenLDAP CSV-Export)

Open Directory Service kann bei Suchergebnissen kennzeichnen, aus welcher Datenquelle ein Treffer stammt.

22.4.1 Wie Sie Open Directory Service aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Applikationen > Open Directory Service**.

3) Klicken Sie im Menübaum auf **Open Directory > Grundeinstellungen**.

4) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie Open Directory Service aktivieren möchten, aktivieren Sie das Kontrollkästchen **Aktiv**.
- Wenn Sie Open Directory Service deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Aktiv**.

5) Klicken Sie auf **Speichern**.

6) Klicken Sie auf **OK**.

7) Klicken Sie auf **OK**.

22.4.2 Wie Sie Open Directory Service neu starten

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.
- Open Directory Service ist aktiviert.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Applikationen > Open Directory Service**.

3) Klicken Sie im Menübaum auf **Open Directory > Wartung**.

4) Klicken Sie auf **Neustart**.

5) Klicken Sie auf **OK**.

22.4.3 Wie Sie das Passwort für Zugriff auf Open Directory Service konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Führen Sie die folgenden Schritte durch, um das Passwort festzulegen, mit welchem Clients, Kommunikationsgeräte und Anwendungen auf Open Directory Service zugreifen können.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Applikationen > Open Directory Service**.

3) Klicken Sie im Menübaum auf **Open Directory > Grundeinstellungen**.

4) Geben Sie das gewünschte **Passwort** ein.

5) Klicken Sie auf **Speichern**.

6) Klicken Sie auf **OK**.

22.4.4 Wie Sie eine externe Datenquelle für Open Directory Service hinzufügen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.
- Die Zugangsdaten der externen Datenbank liegen vor.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Applikationen > Open Directory Service**.

3) Klicken Sie im Menübaum auf **Open Directory > Datenquellen**.

4) Klicken Sie auf **Hinzufügen**.

5) Klicken Sie auf die Registerkarte **Datenbank**.

6) Geben Sie **Name** der Datenquelle ein.

7) Geben Sie eine **Beschreibung** der Datenquelle ein.

8) Wählen Sie in der Aufklappliste **ODBC-Treiber** den gewünschten Typ.

9) Geben Sie in **Server-Adresse der Datenbank** die IPv4-Adresse der Datenbank ein.

10) Geben Sie **Server-Port der Datenbank** ein.

11) Geben Sie **Name der Datenbank** in korrekter Groß-/Kleinschreibung ein.

12) Wenn Sie in der Aufklappliste **ODBC-Treiber** den Typ **Microsoft SQL Server** gewählt haben, geben Sie in Feld **TDS Protokollversion** die TDS Protokollversion ein.

13) Geben Sie **Datenbank-Login** in korrekter Groß-/Kleinschreibung ein.

14) Geben Sie **Datenbank-Passwort** in korrekter Groß-/Kleinschreibung ein.

15) Klicken Sie auf **Prüfe Datenbankzugriff** um den Zugriff zu testen.

16) Klicken Sie auf **OK**.

17) Klicken Sie auf die Registerkarte **Datenzugriff**.

18) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie eine Datenbanktabelle verwenden möchten, klicken Sie auf **Einfache Auswahl - Zugriff auf eine Tabelle**.
- Wenn Sie eine benutzerdefinierte SQL-Abfrage verwenden möchten, klicken Sie auf **Benutzerdefinierte SQL-Abfrage**.

19) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie eine Datenbanktabelle verwenden möchten, klicken Sie **Datenbanktabellen abfragen** und wählen Sie in der Liste **Datenbanktabellen** die gewünschte Tabelle.
- Wenn Sie eine benutzerdefinierte SQL-Abfrage verwenden möchten, geben Sie diese in **SQL-Abfrage** ein.

20) Wenn Sie zur Kontrolle eine Vorschau auf die Daten anzeigen möchten, wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie eine Datenbanktabelle verwenden, klicken Sie auf **Vorschau der Datenbanktabelle** und navigieren Sie in der Vorschau mit Hilfe der entsprechenden Schaltflächen durch die Datensätze.
- Wenn Sie eine benutzerdefinierte SQL-Abfrage verwenden, klicken Sie auf **Vorschau des Abfrageergebnisses** und navigieren Sie in der Vorschau mit Hilfe der entsprechenden Schaltflächen durch die Datensätze.

21) Klicken Sie auf die Registerkarte **Feldzuordnungen**.

> ***INFO:*** Alle Spalten der gewählten Tabelle bzw. alle Spalten welche die benutzerdefinierte SQL-Abfrage zurückliefert, stehen für die Feldzuordnungen zur Verfügung.

22) Klicken Sie auf **Feldzuordnung hinzufügen**.

23) Wählen Sie in der Aufklappliste links jeweils das Feld der externen Datenquelle und in der Aufklappliste rechts in der selben Zeile jeweils das gewünschte zugeordnete Feld im Datenschema von Open Directory Service. Zur Kontrolle wird rechts eine Vorschau auf betreffende Datensätze

angezeigt, durch die Sie mit Hilfe der entsprechenden Schaltflächen navigieren können.

INFO: Das Feld **Identifikationsnummer** muss einem Feld der externen Datenquelle zugeordnet werden, welches eindeutig ist.

24) Wenn Sie eine Zeile von Feldzuordnungen entfernen möchten, klicken Sie links auf das Papierkorb-Symbol.

25) Klicken Sie auf die Registerkarte **Rufnummernkonvertierung**.

26) Aktivieren Sie das Kontrollkästchen **Aktiv**.

27) Klicken Sie auf **Systemeinstellungen auslesen**.

28) Wenn sich die externe Datenbank an einem anderen Standort befindet als das System:

a) Geben Sie die **Länderkennzahl** ein.

b) Geben Sie die **Ortskennzahl** ein.

c) Geben Sie die **Amtskennziffer** ein.

d) Geben Sie **Nationaler Präfix** ein.

e) Geben Sie **Nationaler Präfix** ein.

f) Geben Sie die **Maximale Länge interner Rufnummern** ein.

29) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie eine in der externen Datenquelle eventuell vorhandene Amtskennziffer entfernen möchten, aktivieren Sie das Kontrollkästchen **Amtskennziffer entfernen**.
- Wenn Sie die Amtskennziffer nicht entfernen möchten, deaktivieren Sie das Kontrollkästchen **Amtskennziffer entfernen**.

30) Klicken Sie auf **Speichern**.

31) Klicken Sie auf **OK**.

Nächste Schritte

Starten Sie Open Directory Service neu, damit die Änderung wirksam wird.

Führen Sie eine Vorschau auf das LDAP-Suchergebnis durch.

22.4.5 Wie Sie eine Vorschau auf LDAP-Suchergebnis für Open Directory Service durchführen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Führen Sie die folgenden Schritte durch, um zu kontrollieren, ob ein LDAP-Suchergebnis von Open Directory Service Datensätze in der gewünschten Form und mit dem korrekten Rufnummernformat liefert.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen > Open Directory Service**.
3) Klicken Sie im Menübaum unter **Open Directory > Datenquellen** auf die gewünschte Datenquelle.
4) Klicken Sie auf die Registerkarte **LDAP-Test**.
5) Klicken Sie auf **Test starten**. Unter **LDAP Suchergebnis** wird die Vorschau auf das Suchergebnis angezeigt.

22.4.6 Wie Sie eine externe Datenquelle für Open Directory Service löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen > Open Directory Service**.
3) Klicken Sie im Menübaum auf **Open Directory > Datenquellen**.
4) Klicken Sie im Arbeitsbereich auf die betreffende Datenquelle.
5) Klicken Sie auf **Löschen**.
6) Klicken Sie auf **OK**.

Nächste Schritte

Starten Sie Open Directory Service neu, damit die Änderung wirksam wird.

22.5 XMPP

XMPP (Extensible Messaging and Presence Protocol) ist ein Internetstandard für XML-Routing und wird vor allem für Instant Messaging eingesetzt. XMPP ermöglicht die Einbindung externer Kommunikationspartner für Sofortnachrichten sowie Mapping zwischen Anwesenheitsstatus und XMPP-Status.

XMPP wird von folgenden Clients unterstützt:

- myPortal for Desktop
- myPortal for Outlook

- myAttendant

Externe XMPP-Kommunikationspartner können z. B. Benutzer von Google Talk oder Microsoft Lync Office Communicator sein.

Der integrierte Openfire XMPP-Server wird von extern standardmäßig über Port 5269 adressiert. Die Verbindungen zu anderen XMPP-Servern können mit TLS gesichert werden, sofern diese TLS unterstützen. Zur internen Kommunikation mit Clients dient Port 5222. Die Ports müssen in entsprechenden Firewalls freigegeben sein. XMPP ist im System standardmäßig deaktiviert und kann vom Administrator konfiguriert werden. Die erforderliche Konfiguration von XMPP im jeweiligen Client kann der Teilnehmer durchführen. Externe XMPP-Gateway-Server werden nicht unterstützt. XMPP-IDs externer Kommunikationspartner müssen dem Muster `xmpp:john.public@osbiz.example-for-a-domain.com` entsprechen und können an folgenden Stellen vorhanden sein:

- externes Verzeichnis
- externes Offline-Verzeichnis (LDAP)
- Persönliches Verzeichnis (myPortal for Desktop)
- Outlook-Kontakte (myPortal for Outlook)
  Feld: IM-Adresse
- Favoriten

Verwandte Themen

- Sofortnachrichten (UC Suite)

22.5.1 Wie Sie XMPP konfigurieren

Voraussetzungen

- Das System hat eine Verbindung zum Internet.
- Das System ist im Internet unter einem Namen erreichbar, z. B. `osbiz.example-for-a-domain.com`.
- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Applikationen > WebServices**.

3) Klicken Sie im Menübaum auf **WebServices > XMPP**.

4) Aktivieren Sie das Kontrollkästchen **XMPP Modus ein**.

5) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn es sich um ein Stand Alone System handelt, wählen Sie die Option **XMPP Stand Alone**.
- Wenn es sich um ein vernetztes System handelt, wählen Sie die Option **XMPP in der Vernetzung**.

6) Wenn es sich um ein Stand Alone System handelt oder um ein vernetztes System, das Master ist, geben Sie in **XMPP Domäne** den Namen ein, unter welchem das System im Internet erreichbar ist, in der Form `osbiz.example-for-a-domain.com`.

> ***INFO:*** Die Aktualisierung dieser Daten im Netz kann bis zu 10 Minuten dauern.

7) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie nur gesicherte Verbindungen zu anderen Servern benutzen möchten, aktivieren Sie das Kontrollkästchen **Sichere Verbindungen (TLS) zulassen**.
- Wenn Sie keine gesicherten Verbindungen zu anderen Servern benutzen möchten, deaktivieren Sie das Kontrollkästchen **Sichere Verbindungen (TLS) zulassen**.

8) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

22.6 Application Launcher

Application Launcher ist eine Java-basierte Windows-Anwendung für die anrufbezogene Steuerung von Anwendungen auf Client-PCs von Benutzern von UC Suite. Application Launcher kann z. B. verwendet werden, um in einem CRM-System automatisch das Kontaktformular für den jeweiligen Anrufer zu öffnen.

Application Launcher bietet folgende Leistungsmerkmale:

- Beziehen anrufbezogener Informationen zur Rufnummer (z. B. Rufnummer, Name des Gesprächspartners, Kunden-ID) entweder aus Open Directory Service oder in Verzeichnissen des Systems
- Aufruf von Windows-Anwendungen oder Web-Anwendungen bei ankommenden und gehenden Anrufen
- Übergabe von anrufbezogenen Informationen an Windows-Anwendungen oder Web-Anwendungen
- automatischer Betrieb im Hintergrund bei ankommenden Anrufen
- optionales, konfigurierbares PopUp-Fenster bei ankommenden Anrufen mit anrufbezogenen Informationen und Schaltflächen für Benutzeraktionen
- Anruferliste mit Anruffunktion
- Vorschaufunktionen für Tests während Konfiguration
- einfaches Übernehmen der Konfiguration vom ersten konfigurierten Client in alle weiteren mittels Konfigurationsprofil im System

22.6.1 Voraussetzungen für Application Launcher

Um Application Launcher zu nutzen muss der Client-PC des jeweiligen Benutzers von UC Suite über geeignete Hardware und Software verfügen.

Betriebssystem

Application Launcher kann in Verbindung mit folgenden Betriebssystemen verwendet werden:

- Microsoft Windows 8
- Microsoft Windows 7
- Microsoft Windows Vista

Die Installation erfordert lokale Administrationsrechte auf einem Client-PC, automatische Updates jedoch nicht.

Windows Update

Die PCs benötigen stets den aktuellen Stand aller verfügbaren Updates einschließlich Service Packs.

Zusätzliche Software

Java in der aktuellsten Version (siehe **Service-Center > Applikationen**)

Web Services für Mobiltelefone

Web Services für Mobiltelefone muss im System aktiviert sein für die Systemverbindung. An Firewalls im LAN und an Client-PCs müssen die im System konfigurierten Ports geöffnet sein.

Open Directory Service (optional)

Wenn Application Launcher Daten von Open Directory Service nutzen soll, muss Open Directory Service im System konfiguriert sein. An Firewalls im LAN und an Client-PCs muss der im System konfigurierte Port geöffnet sein.

Verwandte Themen

- Konfiguration von myPortal for Mobile und Mobility Entry

22.6.2 Profil mit Konfigurationsdaten von Application Launcher

Ein Profil mit Konfigurationsdaten von Application Launcher ermöglicht die einfache und schnelle Konfiguration von Application Launcher auf allen Client-PCs.

Das Profil beinhaltet sämtliche Konfigurationsdaten, bis auf die Systemverbindung und die Benutzerdaten. Sobald Application Launcher für einen ersten Benutzer vollständig konfiguriert ist, können Sie als Administrator dessen Profil mit den Konfigurationsdaten von Application Launcher im Kommunikationssystem bereitstellen. Anschließend können alle Benutzer die Konfiguration von Application Launcher durch Importieren dieses Profils durchführen.

22.6.2.1 Wie Sie das Profil mit Konfigurationsdaten von Application Launcher bereitstellen

Voraussetzungen

- Application Launcher ist für einen Benutzer vollständig konfiguriert.
- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Applikationen > OpenScape Application Launcher**.

3) Klicken Sie auf **Durchsuchen** und wählen Sie folgende Datei aus: `C:\Documents and Settings\<Windows User Name>\Application Data\Tray_Tool\profile.xml`.

4) Klicken Sie auf **Öffnen**.

5) Klicken Sie auf **Laden**.

Nächste Schritte

Alle Benutzer können dieses Profil in Application Launcher importieren und dadurch die Konfiguration durchführen.

23 Accounting

Accounting umfasst die Erfassung von Verbindungsdaten, Projektkennzahlen, die Übertragung und Anzeige von Verbindungsdaten sowie Kostenkontrolle und Accounting Tools.

23.1 Verbindungsdaten

Verbindungsdaten umfassen die Erfassung von Verbindungsdaten sowie Projektkennzahlen.

23.1.1 Erfassung von Verbindungsdaten

Das System kann die Verbindungsdaten seiner genutzten Leitungen protokollieren.

Für jede beendete Verbindung bzw. bei jeder kommenden Verbindung wird ein Verbindungsdatensatz aufgezeichnet. Für einen neuen zeitlichen Abschnitt einer Verbindung (z. B. durch Übergabe oder Weiterleitung an einen anderen Teilnehmer) wird ein eigener Verbindungsdatensatz aufgezeichnet. Interne Verbindungen werden nicht protokolliert.

Der Administrator kann für die Erfassung von Verbindungsdaten folgende Optionen aktivieren:

- Erfassung ein bzw. aus
- Verbindungsdauer
- Geldbeträge oder Tarifeinheiten:
  Die Umrechnung von Tarifeinheiten in Geldbeträge erfolgt anhand des konfigurierbaren Tariffaktors (Währungsbetrag pro Tarifeinheit).
- Dezimalformat
  Teilt den Geldbetrag durch 100, um z. B. 6 Cent als 0,06 darzustellen
- Letzte vier Ziffern von Zielrufnummern unterdrücken
- Kommende Verbindungen protokollieren
- Gehende Anrufe ohne Verbindung:
  Hierdurch erhält der Teilnehmer z. B. einen Nachweis für die Nichtannahme eines Anrufs durch den Zielteilnehmer (gekennzeichnet durch Verbindungsdauer 00:00:00). Die Option gilt für ISDN-Verbindungen und für alle Teilnehmer.
- Verbindungsprotokoll
  Protokoll bereits bei Anrufbeginn
- MSN protokollieren
- Ausgabe der LCR Nummer gehend oder der gewählten Rufnummer kommend

- gehend:
  die von LCR tatsächlich zum PSTN gesendete Rufnummer
- kommend:
  die ursprünglich gewählte interne Rufnummer

Entstehen Verbindungskosten bereits vor dem Verbindungsaufbau (wie z. B. in Österreich), werden diese erfasst, unabhängig davon, ob die Protokollierung gehender Anrufe ohne Verbindung aktiviert ist.

Das System berücksichtigt Verbindungen über QSIG-Leitungen nur, wenn für diese eine Leitungskennzahl konfiguriert ist.

Es erfolgt keine Protokollierung bei:

- vorzeitigem Abbruch des Wahlversuchs
- unzulässigen Verbindungen (LCR, Verbotslisten).

Verwandte Themen

- Projektkennzahlen

23.1.1.1 Wie Sie die Erfassung von Verbindungsdaten aktivieren oder deaktivieren

Mit dem Wizard **Gesprächsdatenerfassung** können Sie die Erfassung von Verbindungsdaten aktivieren.

Voraussetzungen

- Sie sind am WBM angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Zentrale Telefonie**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Gesprächsdatenerfassung** zu starten.

4) Wählen Sie eine der folgenden Möglichleiten:

- Wenn Sie die Erfassung von Verbindungsdaten aktivieren möchten, aktivieren Sie das Kontrollkästchen **Gebührenerfassung einschalten**.
- Wenn Sie die Erfassung von Verbindungsdaten deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Gebührenerfassung einschalten**.

5) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

23.1.1.2 Wie Sie die Protokollierung der Verbindungsdauer aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen > Gebühren > Gebühren Ausgabe**.
4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie die Funktion aktivieren möchten, aktivieren Sie das Kontrollkästchen **Anrufdauerprotokollierung ein**.
   - Wenn Sie die Funktion deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Anrufdauerprotokollierung ein**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

23.1.1.3 Wie Sie die Protokollierung von Geldbeträgen oder Tarifeinheiten konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen > Gebühren > Gebühren Ausgabe**.
4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie möchten, dass das System Geldbeträge protokolliert, aktivieren Sie das Kontrollkästchen **Beträge statt Einheiten ausgeben**.
   - Wenn Sie möchten, dass das System Tarifeinheiten protokolliert, deaktivieren Sie das Kontrollkästchen **Beträge statt Einheiten ausgeben**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

23.1.1.4 Wie Sie Tariffaktor, Währung und Rechengenauigkeit konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen > Gebühren > Gebühren Faktoren**.
4) Geben Sie für jede betreffende Richtung in den Feldern **Multiplikator** und **Multipl. ISDN** die entsprechenden Werte ein.
5) Geben Sie im Feld **Währung** am unteren Ende des Formulars den entsprechenden Wert ein.
6) Wählen Sie für jede betreffende Richtung mit dem QSIG-Protokoll in Übereinstimmung mit dem verbundenen Kommunikationssystem eine der folgenden Möglichkeiten:
   - Wenn Währungsbeträge empfangen und gesendet werden sollen, aktivieren Sie das Kontrollkästchen **Währungsbetrag**.
   - Wenn Tarifeinheiten empfangen und gesendet werden sollen, deaktivieren Sie das Kontrollkästchen **Währungsbetrag**.
7) Geben Sie in jeder Zeile mit einer Richtung mit QSIG-Protokoll, welche Tarifeinheiten empfängt und sendet, in **Währung** ein Leerzeichen ein.
8) Wählen Sie aus der Aufklappliste **Rechengenauigkeit** den Eintrag **Keine Nachkommastelle**, **1 Nachkommastelle**, **2 Nachkommastellen**, **3 Nachkommastellen** oder **Über Gebührenimpulse**.
9) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

23.1.1.5 Wie Sie die Protokollierung der letzten vier Ziffern aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen > Gebühren > Gebühren Ausgabe**.
4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie die Funktion aktivieren möchten, aktivieren Sie das Kontrollkästchen **Letzte 4 Ziffern unterdrücken**.
   - Wenn Sie die Funktion deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Letzte 4 Ziffern unterdrücken**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

23.1.1.6 Wie Sie die Protokollierung gehender Anrufe ohne Verbindung aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen > Gebühren > Gebühren Ausgabe**.
4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie die Funktion aktivieren möchten, aktivieren Sie das Kontrollkästchen **Gehend ohne Verbindung**.
   - Wenn Sie die Funktion deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Gehend ohne Verbindung**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

23.1.1.7 Wie Sie die Protokollierung kommender Verbindungen aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen > Gebühren > Gebühren Ausgabe**.
4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie die Funktion aktivieren möchten, aktivieren Sie das Kontrollkästchen **Kommende Gespräche protokollieren**.
   - Wenn Sie die Funktion deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Kommende Gespräche protokollieren**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

23.1.1.8 Wie Sie das Verbindungsprotokoll aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **Grundeinstellungen > Gebühren > Gebühren Ausgabe**.

4) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie die Funktion aktivieren möchten, aktivieren Sie das Kontrollkästchen **Anrufprotokoll ein**.
- Wenn Sie die Funktion deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Anrufprotokoll ein**.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

23.1.1.9 Wie Sie die Protokollierung der MSN aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **Grundeinstellungen > Gebühren > Gebühren Ausgabe**.

4) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie die Funktion aktivieren möchten, aktivieren Sie das Kontrollkästchen **Ausgabe der MSN ein**.
- Wenn Sie die Funktion deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Ausgabe der MSN ein**.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

23.1.1.10 Wie Sie das Dezimalformat aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **Grundeinstellungen > Gebühren > Gebühren Ausgabe**.

4) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie die Funktion aktivieren möchten, aktivieren Sie das Kontrollkästchen **Dezimalformat**.
- Wenn Sie die Funktion deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Dezimalformat**.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

23.1.2 Projektkennzahlen

Projektkennzahlen (PKZ) ermöglichen die projektbezogene Zuordnung von Verbindungsdaten und -kosten. Das System protokolliert hierfür in den entsprechenden Verbindungsdatensätzen die von den Teilnehmern am Telefon eingegebenen Projektkennzahlen.

PKZ wird in Verbindung mit der Erfasung von Verbindungsdaten genutzt und steht jedem Teilnehmer zur Verfügung.

Der Teilnehmer kann eine PKZ am Telefon vor Wahlbeginn oder nach Wahlende eingeben. Die Wahl aus einem Client bei aktivierter PKZ ist nicht möglich.

Eine während einer Konferenz mit externen Teilnehmern eingegebene PKZ wird allen beteiligten Verbindungen bzw. Leitungen zugeordnet.

Der Administrator kann einstellen, ob eine PKZ für die Wahlwiederholung eichert werden kann.

Das persönliche Telefonbuch kann in einem Eintrag die Kennzahl für das Leistungsmerkmal PKZ + eine PKZ + eine Rufnummer gemeinsam speichern.

PKZ-Eingabeverfahren

Der Administrator legt das PKZ-Eingabeverfahren im LCR-Wahlplan fest:

- Erzwungen
  Die PKZ muss vor Verbindungsbeginn (vor oder nach Belegen einer Richtung) eingegeben werden.
- Freiwillig
  Die PKZ kann freiwillig vor Verbindungsbeginn eingegeben werden. An IP-Telefonen Clients ist die Eingabe zusätzlich während einer Verbindung möglich, auch kommend.

PKZ-Prüfverfahren

Das System kann die Gültigkeit einer eingegebenen PKZ auf folgende Arten prüfen:

- Listenprüfung
  Gültig sind nur vordefinierte PKZ. Nach Eingabe einer gültigen PKZ kann der Teilnehmer unmittelbar weiter wählen. Das System weist eine ungültige PKZ ab. Im Display erscheint "Falscher Eintrag" und es ertönt ein negativer Quittungston.
- Prüfung der Stellenzahl
  Gültig sind alle theoretisch möglichen PKZ mit der konfigurierten Stellenanzahl. Nach Eingabe einer gültigen PKZ durch den Teilnehmer kann unmittelbar weiter gewählt werden.
- Keine Prüfung
  Die PKZ wird nicht auf ihre Gültigkeit hin überprüft. PKZ mit weniger als 11 Stellen muss der Teilnehmer durch Wahl von “#” von den weiteren gewählten Ziffern abgrenzen. Bei ISDN-Endgeräten erfordert diese Variante immer 11-stellige PKZ, ansonsten wird die Wahl nicht ausgeführt.

Wenn der Teilnehmer während einer Verbindung feststellt, dass die einer Verbindung zugeordnete PKZ nicht korrekt ist, kann er eine andere eingeben. Das System überschreibt die aktuell gesetzte PKZ. Die Erfassung von Verbindungsdaten erstellt nach jedem Segment einen Verbindungsdatensatz. Daher werden zuvor abgeschlossene Verbindungsabschnitte mit der alten PKZ gekennzeichnet.

Verwandte Themen

- Erfassung von Verbindungsdaten

23.1.2.1 Wie Sie eine Projektkennzahl konfigurieren

Mit dem Wizard **Gesprächsdatenerfassung** können Sie Projektkennzahlen konfigurieren.

Voraussetzungen

- Sie sind am WBM angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Zentrale Telefonie**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Gesprächsdatenerfassung** zu starten.

4) Geben Sie im Bereich **Projekt-Kennzahlen** in den Eingabefeldern die Projektkennzahlen in der vom Wizard beschriebenen Weise ein.

5) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

23.1.2.2 Wie Sie ein PKZ-Prüfverfahren konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **Grundeinstellungen > Gebühren > Gebühren Projekt Kennzahlen**.

4) Wählen Sie in der Zeile der betreffenden PKZ-Liste in der Aufklappliste **Prüfverfahren** den gewünschten Eintrag: **Keine Prüfung**, **Listen-Prüfung** oder **Prüfung der Stellenzahl**.

a) Wählen Sie ggf. in der Aufklappliste **Anzahl der zu prüfenden Stellen** den gewünschten Wert.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

23.1.2.3 Wie Sie Wahlwiederholung mit PKZ aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **Grundeinstellungen > System > System Flags**.

4) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie die Funktion aktivieren möchten, aktivieren Sie das Kontrollkästchen **Wahlwiederholung mit PKZ**.
- Wenn Sie die Funktion deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Wahlwiederholung mit PKZ**.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

23.2 Anzeige und Übertragung von Verbindungsdaten

Die Anzeige und Übertragung von Verbindungsdaten umfasst verschiedene Möglichkeiten der Anzeige im Display der Systemtelefone und zur Dateiübertragung.

23.2.1 Übermittlung von Geldbeträgen (nicht für USA)

Das System kann den vom Netzbetreiber übermittelten Geldbetrag zur aktuellen externen Verbindung im Display des Telefons anzeigen.

Der Netzbetreiber muss die Übermittlung von Geldbeträgen beim Leistungsmerkmal Advice Of Charge (AOC-D oder AOC-S) unterstützen. Das System kumuliert die Beträge der entsprechenden Tarifeinheiten.

Der Geldbetrag kann grundsätzlich zu folgenden Zeiten übermittelt werden:

- bei Verbindungsbeginn und gegebenenfalls während der Verbindung (AOC-S)
- laufend während der Verbindung (AOC-D)

Über den Parameter Rechengenauigkeit kann der Administrator Ungenauigkeiten bei der Aufzeichnung der Verbindungsdaten vermeiden. Die Rechengenauigkeit bestimmt:

- die Anzahl der Nachkommastellen für die Verbindungsdatenauswertung (kleinster Geldbetrag)
- die maximale Summe der kumulierten Geldbeträge.

Die eingestellte Rechengenauigkeit muss mindestens jener von ISDN entsprechen. Falls die maximal möglichen drei Nachkommastellen nicht ausreichen, wird automatisch gerundet. Rechengenauigkeit kann folgende Werte annehmen:

Rechengenauigkeit	kleinster Geldbetrag	größter Geldbetrag
keine Nachkommastellen	1	ca. 4,3 Milliarden
1 Nachkommastelle	0,1	ca. 430 Millionen
2 Nachkommastellen (z. B. für Euro)	0,01	ca. 43 Millionen
3 Nachkommastellen (z. B. für Engl. Pound Sterling)	0,001	ca. 4,3 Millionen

23.2.1.1 Wie Sie die Übermittlung von Geldbeträgen konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **Grundeinstellungen > Gebühren > Gebühren Faktoren**.

4) Wählen Sie je gewünschter Richtung in der Aufklappliste **Gebührenmode** den Eintrag **während der Verbindung**, **am Ende der Verbindung**, **während / am Ende der Verbindung** oder **keine Gebühren**.

5) Wählen Sie in der Aufklappliste **Rechengenauigkeit** am unteren Ende des Formulars die Anzahl der zu berücksichtigenden Nachkommastellen.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

23.2.2 Anzeige der Verbindungskosten am Telefon

Das System kann Informationen zu den Kosten einer bestehenden externen Verbindung im Display des Telefons als Geldbetrag anzeigen.

Das System kumuliert die Beträge der entsprechenden Tarifeinheiten. Der Geldbetrag berechnet sich aus den Tarifeinheiten und dem konfigurierten Tarifaktor. Der Service-Provider muss das Leistungsmerkmal Advice Of Charge (AOC) unterstützen.

Die Information zu den Verbindungskosten kann zu folgenden Zeiten übermittelt werden:

- Bei Verbindungsbeginn und gegebenenfalls während der Verbindung (AOC-S)
- Während der Verbindung (AOC-D)
- Bei Verbindungsende (AOC-E)

Bei Verbindungsende zeigt das Display die endgültigen Verbindungskosten für ca. 5 Sekunden an, sofern der Teilnehmer nicht eine andere Aktion startet.

Beim Makeln werden immer die Verbindungskosten für die aktuelle Verbindung angezeigt.

Bei nicht erfolgreicher Übergabe vor Melden wird der Gesamtbetrag angezeigt und berechnet.

Einem Teilnehmer, dem eine Verbindung übergeben wird, werden nur die Verbindungskosten ab diesem Zeitpunkt belastet und angezeigt.

23.2.3 Anzeige der Verbindungsdauer am Telefon

Das System kann die Dauer gehender und kommender externer Verbindungen im Display des Telefons anzeigen.

Das Format ist HH:MM:SS.

Ist die Verbindungsdaueranzeige deaktiviert, zeigt das Display am Telefon stattdessen die Information zu den Verbindungskosten des PSTN an. Ist keine Information zu den Verbindungskosten vorhanden, zeigt das Display die Rufnummer des Gesprächspartners, sofern bekannt.

23.2.3.1 Wie Sie die Anzeige der Verbindungsdauer aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **Grundeinstellungen > System > Display**.

4) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie die Funktion aktivieren möchten, aktivieren Sie das Kontrollkästchen **Gesprächsdauer anzeigen**.
- Wenn Sie die Funktion deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Gesprächsdauer anzeigen**.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

23.2.4 Übertragung von Verbindungsdaten

Das System kann Verbindungsdaten in einer Datei über HTTPS übertragen.

Sie können übertragene Datei mit einem geeigneten Programm auswerten.

Eine fortlaufende Ausgabe der Verbindungsdaten ist ausschließlich via CSTA möglich.

Der Administrator kann für Verbindungsdaten zwischen folgenden Formaten (ASCII 8-bit) wählen:

- Komprimiertes Format
- Unkomprimiertes Format

Komprimiertes Format, Standard

Ein Verbindungsdatensatz im komprimierten Format enthält folgende durch | getrennte Felder, wobei CRLF jeden Verbindungsdatensatz abschließt:

Feldposition	Länge	Beschreibung
1	8	Datum bei Verbindungsende
2	8	Uhrzeit bei Verbindungsende
3	3	Belegte Amtsleitungsnummer
4	16	Interne Teilnehmernummer
5	8	Klingeldauer der kommenden Verbindung
6	8	Dauer der Verbindung
7	max. 25	gewählte oder empfangene externe Rufnummer

Feldposition	Länge	Beschreibung
8	11	Tarifeinheit/Betrag
9	2	Zusätzliche Informationen, (z. B. kommend, gehend, übergebene Verbindung, Konferenz, DISA, Kosten für Verbindungsaufbau)
10	max. 11	PKZ
11	max. 11	nur bei Mehrgeräteanschluss: benutzte MSN
12	6	Access Code LCR, Amtskennzahl
13	2	Benutzte LCR Route, Wahlregel
14	25	Gewählte oder empfangene Rufnummer (optional)

Beispiele für Verbindungsdatensätze:

- abgehende Verbindung:
  `13.02.13|14:18:02|201|33388|00:02|00:00:07|0123456789||1||||||`
- ankommende Verbindung:
  `13.02.13|14:28:02|202|33388|00:05|00:00:12|0123456789||1|||||`

Komprimiertes Format, USA-spezifisch

Ein Verbindungsdatensatz im komprimierten Format enthält folgende durch | getrennte Felder, wobei CRLF jeden Verbindungsdatensatz abschließt:

Feldposition	Länge	Beschreibung
1	8	Datum bei Verbindungsende
2	8	Uhrzeit bei Verbindungsende
3	3	Belegte Amtsleitungsnummer
4	16	Interne Teilnehmernummer
5	8	Klingeldauer der kommenden Verbindung
6	8	Dauer der Verbindung
7	max. 25	gewählte oder empfangene externe Rufnummer
8	11	Tarifeinheit/Betrag
9	2	Zusätzliche Informationen, (z. B. kommend, gehend, übergebene Verbindung, Konferenz, DISA, Kosten für Verbindungsaufbau)
10	max. 11	PKZ
11	max. 11	nur bei Mehrgeräteanschluss: benutzte MSN
12	6	Access Code LCR, Amtskennzahl
13	2	Benutzte LCR Route, Wahlregel
14	2	PRI Nodal Service

Feldposition	Länge	Beschreibung
15	1	PRI WATS band
16	3	PRI CIC
17	25	Gewählte oder empfangene Rufnummer (optional)

Unkomprimiertes Format

Das unkomprimierte Format eignet sich für Ausdrucke. Außerdem wird eine Kopfzeile und Seitenvorschub ausgegeben. Ein Verbindungsdatensatz im komprimierten Format enthält folgende durch | getrennte Felder:

Feldposition	Zeichenposition, Länge	Beschreibung
1	1-8 (8)	Datum bei Verbindungsende: TT.MM.JJ (TT = Tag: Wertebereich 01 ... 31, MM = Monat: Wertebereich 01 ... 12, JJ = Jahr: Wertebereich 00 ... 99)
2	9-16 (8)	Uhrzeit am Ende des Verbindungsabschnittes bzw. eines nicht beantworteten kommenden Rufes: hh:mm:ss (hh = Stunden: Wertebereich 00 ... 23, mm = Minuten: Wertebereich 00 ... 59, ss = Sekunden: Wertebereich 00 ... 59)
3	17-19 (3)	Leitung: Leitungsnummer Wertebereich 1 ... 250
4	20-35 (16)	Teilnehmer: interne Teilnehmernummer Bei nicht beantworteten Anrufen wird immer der zuletzt gerufene Teilnehmer ausgegeben (z. B. Sammelanschluss, Anrufumleitung, Rufweiterschaltung). Beim Gruppenruf ist dies der zuletzt eingetragene Teilnehmer. Bei abgefragten Rufen wird der Teilnehmer angegeben, der den Ruf angenommen hat. Ein programmiertes RNR-Präfix (nur bei Vernetzung) wird nicht ausgegeben. Wurde die interne Nummerierung auf einen max. 7-stelligen Rufnummernplan umgewertet, wird die umgewertete Rufnummer ausgegeben. Der internen Teilnehmerrufnummer kann eine maximal 7-stellige Knotenrufnummer vorangestellt werden. Ist die Summe aus Knotenrufnummer und Teilnehmerrufnummer größer als 7, so werden nur die letzten 7 Ziffern der Nummer ausgegeben.
5	36-40 (5)	Rufdauer einer kommenden Verbindung: mm:ss (mm = Minuten: Wertebereich 00 ... 59, ss = Sekunden: Wertebereich 00 ... 59) Die Anzeige erfolgt bei allen kommenden Rufen, sofern im System die Ausgabe der "Rufdauer" konfiguriert ist. Bei einem Überlauf des Zählers (Dauer > 59:59) erfolgt die Ausgabe von "59:59". Dies kann z. B. bei einer Datums- oder Uhrzeitumstellung während des Betriebs der Anlage vorkommen. Bei einem kommenden Ruf auf einen besetzten Teilnehmer hat die Rufdauer den Wert "00:00".

Feldposition	Zeichenposition, Länge	Beschreibung
6	41-48 (8)	Dauer der Verbindung bzw. des Verbindungsabschnittes: hh:mm:ss (hh = Stunden: Wertebereich 00 ... 23, mm = Minuten: Wertebereich 00 ... 59, ss = Sekunden: Wertebereich 00 ... 59) Ist bei einem ankommenden Anuf keine Verbindung zustande gekommen, werden Leerzeichen ausgegeben. Bei einem Überlauf des Zählers (Dauer > 23:59:59) erfolgt die Ausgabe von "23:59:59".
7	49-73 (25)	Gewählte oder, wenn vorhanden, die empfangene externe Rufnummer: nnnnnnnnnnnnnnnnnnnnnnnnn (n = gewähltes oder empfangenes Zeichen: Wertebereich 0 ... 9, *, #, ?) Die Ausgabe erfolgt bei kommenden und gehenden Rufen, sofern vorhanden. Bei gehenden Rufen wird die gewählte Rufnummer bzw. wenn vorhanden, die über COLP übermittelte Rufnummer angezeigt. Bei aktiver Datenschutzfunktion werden die letzten 4 gewählten Zeichen durch "????" ersetzt. Ist keine Information über die Rufnummer vorhanden, werden Leerzeichen ausgegeben.
8	74-84 (11)	Tarifeinheiten für einen Verbindungsabschnitt: zzzzzzzzzzz (z = Ziffer: Wertebereich 0 ... 9) Es kann zwischen Tarifeinheiten und Geldbeträgen gewählt werden. Die Umrechnung der Tarifeinheiten in Geldbeträge erfolgt anhand des Tariffaktors, der als Währungsbetrag (inklusive eines notwendigen Aufschlags) pro Tarifeinheit definiert ist. Für die Einstellung des Tariffaktors gilt: • mit Rechengenauigkeit: Tariffaktor = 100% + evtl. notwendiger Aufschlag • ohne Rechengenauigkeit: Tariffaktor = Betrag/Einheit + evtl. notwendiger Aufschlag In Abhängigkeit von der Rechengenauigkeit erfolgt die Erfassung der Verbindungskosten mit oder ohne Aufschlag. Die Ausgabe erfolgt immer, wenn für den Verbindungsabschnitt Verbindungskosten anfallen (z. B. auch bei übergebenen Verbindungen).

Feldposition	Zeichenposition, Länge	Beschreibung
9	85-86 (2)	Informationselement: zusätzliche Information Wertebereich 0 ... 9 Bedeutung: • 1 = kommende Verbindung (Voice / 3.1 kHz Audio Call) • 2 = gehende Verbindung (Voice / 3.1 kHz Audio Call) • 3 = kommende Verbindung (Sonstige Services) • 4 = gehende Verbindung (Sonstige Services) • 5 = kommende Verbindung weitervermittelt • 6 = gehende Verbindung weitervermittelt • 7 = int/ext/ext Konferenz mit kommender Verbindung / Transit durch Übergabe nach extern • 8 = Konferenz mit gehender Verbindung / Transit durch Übergabe nach extern • 9 = gehende Verbindung über Anrufumleitung zu externem Ziel • 0 = Verbindungs-Info (Ruferliste), wird sofort bei Eintreffen eines kommenden Anrufes ausgegeben (Ausgabe kann unterdrückt werden). Kann z. B. für eine Datenbanksuche von einem PC genutzt werden. Bei mehreren gerufenen Teilnehmern wird für jeden einzelnen Teilnehmer eine Zeile ausgegeben (ohne Rufdauer, Verbindungsdauer und Gebühreninfo). • +20 = Offset als Kennung für Kosten für den Verbindungsaufbau (ohne Verbindungsdauer) • +30 = Offset als Kennung für einen Folgedatensatz bei – Verbindungsdauer > 24 h. – zusammenhängenden Verbindungsabschnitten mit gleicher Leitungs-/Teilnehmernummer (z. B. nach dem Übergeben einer Verbindung, nach dem Aufheben einer Konferenz). • +40 = Offset für einen Datensatz mit Transitkennung (durch eine Nebenstelle der Unteranlage). Kann in Kombination mit Offset +30 auftreten. • +50 = Offset als Kennung für DISA-Verbindungen • +70 = Kombination der Offsets +30 und +40
10	87-97 (11)	Vom Benutzer für diese Verbindung eingegebene Projektkennzahl PKZ: pppppppppp (p = Ziffer der PKZ: Wertebereich 0 ... 9) Fehlende Ziffern werden durch Leerzeichen ersetzt.

Feldposition	Zeichenposition, Länge	Beschreibung
11	98-108 (11)	Benutzte MSN: mmmmmmmmmmm (m = Ziffer der MSN: Wertebereich 0 ... 9) Die Anzeige erfolgt, sofern der Teilnehmer eine MSN-Taste programmiert hat. Bei gehenden Verbindungen eines MULAP-Teilnehmers wird die Rufnummer der belegten MULAP ausgegeben. Fehlende Ziffern werden durch Leerzeichen ersetzt.
12	109-113 (5)	Benutzte Belegungskennzahl, Access Code: bbbbb (b = Ziffer der Belegungskennzahl: Wertebereich 0 ... 9)
13	114-115 (2)	Benutzte LCR-Route: rr (r = Ziffer der gewählten Route: Wertebereich 0 ... 9)

Kommunikationsablauf

Die Übertragung von Verbindungsdaten kann angefordert werden (Download Request), woraufhin das System entsprechend reagiert (Download Response).

Anschließend kann die Löschung von Verbindungsdaten angefordert werden (Delete Request), woraufhin das System entsprechend reagiert (Download Response).

Download Request - Definition

Element	Inhalt
HTTP header	Request method = GET
URL	https://<IP-Adresse des Systems>/management/portlet
Parameter	portlet=hipath-accountingdownload::HiPathAccountingDownloadPortlet
	entity=accounting
	action=get
	username=<username>
	password=<password>

Beispiel:

```
https://192.148.108.151/management/portlet/?portlet=hipath-
accountingdownload::HiPathAccountingDownload-
Portlet&entity=accounting&action=get&username=xbert@system&
password=not4u;-)
```

Download Response - Definition

Element	Inhalt
HTTP header	ContentType = "text/plain"
Parameter	attachment filename = "<charging file>"
	data=<content of the charging file>

Response-Code	Bedeutung
SC_OK(200)	erfolgreich
SC_BAD_REQUEST(400)	fehlender Parameter in Request
SC_UNAUTHORIZED(401)	Anmeldung fehlgeschlagen oder username bzw. password falsch
SC_INTERNAL_SERVER_ERROR(500)	interner Fehler

Delete Request - Definition

Element	Inhalt
HTTP header	Request method = POST
URL	https://<IP-Adresse des Systems>/management/portlet
Parameter	portlet=hipath-accountingdownload::HiPathAccountingDownloadPortlet
	entity=accounting
	action=delete
	username=<username>
	password=<password>

Beispiel:

```
https://192.148.108.151/management/portlet/?portlet=hipath-
accountingdownload::HiPathAccountingDownload-
Portlet&entity=accounting&action=delete&username=xbert@syst
em&password=not4u;-)
```

Delete Response - Definition

Response-Code	Bedeutung
SC_OK(200)	erfolgreich
SC_BAD_REQUEST(400)	fehlender Parameter in Request
SC_UNAUTHORIZED(401)	Anmeldung fehlgeschlagen oder username bzw. password falsch
SC_INTERNAL_SERVER_ERROR(500)	interner Fehler

Verwandte Themen

- Accounting-Tools

23.2.4.1 Wie Sie das Format auswählen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen > Gebühren > Gebühren Ausgabe**.
4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie das Komprimierte Format wünschen, aktivieren Sie das Kontrollkästchen **Komprimiertes Ausgabeformat**.
   - Wenn Sie das Unkomprimierte Format wünschen, deaktivieren Sie das Kontrollkästchen **Komprimiertes Ausgabeformat**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

23.2.4.2 Wie Sie die Übertragung von Verbindungsdaten über HTTPS aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen > Gebühren > Gebühren Ausgabe**.
4) Wählen Sie in der Aufklappliste **Ausgabe** eine der folgenden Möglichkeiten:
   - Wenn Sie das Leistungsmerkmal aktivieren möchten, wählen Sie den Eintrag **HTTPS**.
   - Wenn Sie das Leistungsmerkmal deaktivieren möchten, wählen Sie den Eintrag **Keine**.
5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

23.3 Kostenkontrolle

Kostenkontrolle umfasst die Leistungsmerkmale Hinweis auf teure Verbindungswege und Schutz vor Gebührenbetrug.

23.3.1 Hinweis auf teure Verbindungswege

Ist ein Anrufziel momentan nicht über den preisgünstigsten Verbindungsweg erreichbar, kann das Telefon dem Teilnehmer einen Hinweis auf den teureren Verbindungsweg geben.

Der Teilnehmer kann so entscheiden, ob er die Verbindung trotz des teureren Verbindungsweges zu diesem Zeitpunkt führen will. Der Hinweis kann auf verschiedene Weise erfolgen:

- Text im Display
- Ton
- Text im Display und Ton

Das System weist auf den teuren Verbindungsweg hin, wenn in der Wegetabelle eine entsprechende Warnung konfiguriert ist und es nicht die Richtung von Index 1 der Wegetabelle benutzt.

Der Hinweis im Display wird nur angezeigt, wenn für die zugehörige Wahlregel kein Name konfiguriert ist. Ist ein Name konfiguriert, wird dieser angezeigt.

23.3.1.1 Wie Sie einen Hinweis auf einen teuren Verbindungsweg konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > LCR**.

3) Klicken Sie im Menübaum auf **Routing > LCR > Wegetabelle** und auf die betreffende Wegetabelle.

4) Wählen Sie für jeden teuren Verbindungsweg (Spalte **Richtung**) in der Aufklappliste **Warnung** den gewünschten Eintrag: **Ton**, **Display** oder **Display + Ton**.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

23.3.2 Schutz vor Gebührenbetrug

Das System kann Verbindungen überwachen, um einen potenziellen Gebührenbetrug zu erkennen (Toll Fraud Monitoring). Dies betrifft Verbindungen, die sowohl eine Amtsleitung ankommen als auch über eine Amtsleitung abgehen.

Der erste Teilnehmer signalisiert die Überschreitung der konfigurierten Verbindungsdauer und ermöglicht so, die Verbindung bei Bedarf zu trennen. Als Administrator können Sie konfigurieren ob bzw. nach welcher Verbindungsdauer eine derartige Verbindung signalisiert werden soll.

23.3.2.1 Wie Sie den Schutz vor Gebührenbetrug aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **Grundeinstellungen > System > Zeitparameter**.

4) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie Schutz vor Gebührenbetrug aktivieren möchten, wählen Sie für **Timer für Toll Fraud Monitoring** in der Aufklappliste **Basis** den gewünschten Eintrag und geben Sie im Feld **Faktor** einen von 255 abweichenden Wert ein. **Basis** * **Faktor** ergibt dann die Verbindungsdauer, nach welcher eine potenziell betrügerische Verbindung signalisiert wird.
- Wenn Sie Schutz vor Gebührenbetrug deaktivieren möchten, geben Sie für **Timer für Toll Fraud Monitoring** im Feld **Faktor** 255 ein.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

23.4 Accounting-Tools

Accounting Tools bietet Accounting Manager und Teledata Office.

Verwandte Themen

- Service Center – Dokumente
- Übertragung von Verbindungsdaten

23.4.1 Accounting Manager

Accounting Manager ist eine Windows-Anwendung zum Abruf von Verbindungsdaten über HTTPS und zu deren Auswertung in Tabellen und Grafiken.

Accounting Manager beinhaltet eine eigene Dokumentation. Accounting Manager ruft Verbindungsdaten von einzelnen Netzknoten ab. Sie können Accounting Manager auch zum Testen der Schnittstellefür Verbindungsdaten verwenden. Sie können Accounting Manager im **Service Center** des WBM herunterladen. Accounting Manager erfordert lokale Administrationsrechte und die Aktivierug von TLS 1.0 in Microsoft Internet Explorer.

23.4.2 Teledata Office

Teledata Office ist eine Windows-Anwendung für die Auswertung von Verbindungsdaten.

24 Maintenance

Das System bietet vielfältige Maintenance-Möglichkeiten. Dazu gehören das Ändern von Telefonie-Einstellungen, das Sichern und Wiederherstellen der Konfigurationsdaten, das Aktualisieren der Software durch Update und Upgrade und Restart-/Reload-Funktionen. Darüber hinaus stehen Funktionen zur Statusermittlung, Überwachung und Wartung zur Verfügung. Durch verschiedene Remote Services ist ein Fernzugriff auf das System möglich.

Wartung des UC Booster Servers

Wird zusätzlich zum Kommunikationssystem ein UC Booster Server betrieben, so bietet auch der UC Booster Server einige Maintenance-Möglichkeiten. Für die Wartung des UC Booster Servers gibt der Administrator beim Aufruf des WBM nicht die IP-Adresse des Kommunikationssystems an, sondern die IP-Adresse des Linux-Servers.

24.1 Telefonie-Konfiguration

Das Kommunikationssystem bietet verschiedene Konfigurationsmöglichkeiten für Telefonie, z. B. Datum und Uhrzeit, SNTP, Kundenindividuelle Displayanzeige, und Wartemusik.

24.1.1 Datum und Uhrzeit

Das Kommunikationssystem enthält eine Systemuhr mit Datum und Uhrzeit. myPortal for Desktop und jedes Display eines Endgerätes zeigt diese Systemzeit.

Sie können die Systemzeit grundsätzlich auf folgende Weise festlegen bzw. synchronisieren:

- Über einen Zeitserver mittels SNTP
- Über eine ISDN-Amtsleitung durch einen gehenden Anruf
- Durch manuelle Einstellung

Nach Aktivierung eines SNTP-Servers ist keine systemindividuelle Einstellung der Systemzeit mehr möglich.

Sollte ein SNTP-Server einmal nicht erreichbar sein und HFA-Systemtelefone eine andere Zeitquelle als das System nutzen, so kann die dort angezeigte Zeit von der Systemzeit abweichen.

Eine nach dem Anlagenhochlauf manuell eingestellte Systemzeit wird immer beim ersten gehenden ISDN-Gespräch durch die ISDN-Zeitinformation überschrieben, vorausgesetzt, der Netzbetreiber übermittelt diese Information. Liegt bei laufender Anlage die Differenz einer manuell eingestellten Systemzeit

zur ISDN-Zeitinformation zwischen 2 und 70 Minuten, wird die ISDN-Zeitinformation übernommen. Anderenfalls wird die manuell eingestellte Systemzeit beibehalten.

Für die Darstellung des Datums im Telefondisplay kann der Administrator eines der folgenden Formate auswählen. Das Format ist zusätzlich abhängig vom Typ des Telefons:

Datumformat	OpenStage	OptiPoint 410, OptiPoint 420
Europa	Di 20.11.07	20. NOV 07
USA	Di 11/20/07	Di NOV 20.07
International1	Di 20.11.07	DI 20 NOV 07
International2	Di 20.11.07	DI 20.11.07

Wenn Sie als Administrator versehentlich ein Datum vor 2007 einstellen, können Sie anschließend nicht mehr auf das WBM zugreifen. Dies ist erst nach einem Restart wieder möglich, der das Datum auf 01.01.2007 zurücksetzt.

24.1.1.1 Wie Sie Datum und Uhrzeit manuell konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Führen Sie die folgenden Schritte durch, wenn das System Datum und Uhrzeit und weder über digitale Amtsleitungen noch über SNTP bezieht.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbereich auf **Telephony Server > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **Grundeinstellungen > Datum und Uhrzeit > Datum und Uhrzeit**.

4) Geben Sie **Datum und Uhrzeit** ein.

5) Klicken Sie auf **Übernehmen**.

6) Klicken Sie auf **Abmelden**.

7) Melden Sie sich am WBM ab und erneut an.

24.1.1.2 Wie Sie die Zeitzone einstellen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbereich auf **Telephony Server > Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen > Datum und Uhrzeit > Zeitzonen-Einstellungen**.
4) Wählen Sie in der Aufklappliste die **Zeitzone**.
5) Klicken Sie auf **Übernehmen**.
6) Melden Sie sich am WBM ab und erneut an.

24.1.1.3 Wie Sie das Datumsformat konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbereich auf **Telephony Server > Grundeinstellungen**.
3) Klicken Sie im Menübaum auf **Grundeinstellungen > System > Display**.
4) Wählen Sie in der Aufklappliste das **Datumsformat**.
5) Klicken Sie auf **Übernehmen**.

24.1.2 SNTP

Über SNTP können Sie Datum und Uhrzeit Ihrer Systeme netzweit mit NTP-Zeitservern synchronisieren.

SNTP (Simple Network Time Protocol) ist eine vereinfachte Version des NTP (Network Time Protocol), ein Standard zur Synchronisierung von Datum und Uhrzeit über paketbasierte Kommunikationsnetze. Um Datum und Uhrzeit zu synchronisieren, benötigt Ihr System eine Verbindung zu einem NTP-Server. Dieser kann sich in Ihrem lokalen Netzwerk oder im Internet befinden. Im Internet gibt es frei zugängliche NTP-Server, aus denen Sie sich einen in Ihrer Zeitzone gelegenen auswählen können. Beachten Sie die Nutzungsbedingungen des entsprechenden Servers und fragen Sie um Erlaubnis, wenn dies nötig ist.

24.1.2.1 Wie Sie Datum und Uhrzeit von einem SNTP-Server beziehen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbereich auf **Telefonie > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **Grundeinstellungen > Datum und Uhrzeit > SNTP-Einstellungen**.

4) Geben Sie **IP-Adresse / DNS-Name des externen Zeitservers** ein, z. B. `0.de.pool.ntp.org`.

5) Wählen Sie in der Aufklappliste **Administrativer Betriebszustand des SNTP-Servers** den Eintrag **Aktiviert**.

6) Wählen Sie in der Aufklappliste **Pollzeit für externen Zeitserver** das gewünschte Zeitintervall für das Beziehen von Datum und Uhrzeit vom SNTP-Server.

7) Klicken Sie auf **Übernehmen**.

8) Melden Sie sich am WBM ab und erneut an.

24.1.3 Telefon-Logos

Systemtelefone mit Display können ein kundenindividuelles Logo als Hintergrund der Telefonie-Oberfläche anzeigen.

Als Administrator können Sie Telefon-Logos für Systemtelefone mit Display importieren, zuweisen oder aus dem System löschen. Unterschiedliche Typen von Systemtelefonen können unterschiedliche Telefon-Logo verwenden.

24.1.3.1 Wie Sie ein Telefon-Logo ins System laden

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.
- Die Bilddatei mit dem Telefon-Logo erfüllt die Voraussetzungen:

	OpenStage 40	OpenStage 60, OpenStage 80
Format	BMP	JPEG
Farbe	monochrom	monochrom oder farbig
Bildgröße (Pixel)	144 x 32	240 x 71
Dateigröße max. (Byte)	702	30k

- Sie haben Zugriff auf die Bilddatei mit dem Telefon-Logo im Dateisystem des Administrations-PCs.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung > Software-Image**.
3) Klicken Sie im Menübaum auf **Telefon-Logo-Images > Laden**.
4) Klicken Sie auf **Durchsuchen**, um eine entsprechende Bilddatei auszuwählen.
5) Klicken Sie auf **Laden**.

24.1.3.2 Wie Sie ein Telefon-Logo an Systemtelefone verteilen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung > Software-Image**.
3) Klicken Sie im Menübaum auf **Telefon-Logo-Images > Verteilen**.
4) Aktivieren Sie in der Zeile des zu verteilenden Telefon-Logos das Kontrollkästchen **Verteilen**.
5) Wählen Sie in der Aufklappliste **An Workpoints folgenden Typs verteilen** den gewünschten Systemtelefontyp aus.
6) Klicken Sie auf **Übernehmen**.

24.1.3.3 Wie Sie ein Telefon-Logo löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.
- Sie haben Zugriff auf die Bilddatei mit dem Telefon-Logo im Dateisystem des Administrations-PCs.

Um ein Telefon-Logo aus dem Kommunikationssystem zu löschen führen Sie folgende Schritte durch:

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung > Software-Image**.

3) Klicken Sie im Menübaum auf **Telefon-Logo-Images > Laden**.

4) Aktivieren Sie in der Zeile des zu löschenden Telefon-Logos das Kontrollkästchen **Löschen**.

5) Wenn Sie weitere Telefon-Logos löschen wollen, wiederholen Sie den vorherigen Schritt.

6) Klicken Sie auf **Löschen**. Alle markierten Telefon-Logos werden aus dem Kommunikationssystem gelöscht.

24.1.4 Kundenindividuelle Displayanzeige

Kundenindividuelle Displayanzeige ermöglicht die Anzeige z. B. des Firmennamens im Display von Systemtelefonen im Ruhezustand.

Veränderbar ist ausschließlich der rechte Teil (max. 18 Zeichen) der zweiten Displayzeile, der standardmäßig mit „OpenScape“ belegt ist. Der Text wird linksbündig zum Datum eingerückt, soweit die Länge des Textes dies zulässt:

```
16:30       FR 29.FEB 08
123456  Hotel zur Post >
```

24.1.4.1 Wie Sie die kundenindividuelle Displayanzeige (System-Name) ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **Grundeinstellungen > Gateway**.

4) Geben Sie im Feld **System-Name** den anzuzeigenden Namen ein.

> ***INFO:*** Verwenden Sie keine anderen Zeichen als A-Z, a-z und 0-9.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.1.5 Mehrsprachige Textausgabe

Die Sprache für Displaymeldungen lässt sich systemweit oder auch teilnehmerindividuell auswählen.

Verfügbare Sprachen: Chinesisch, Dänisch, Deutsch, Englisch, Estnisch, Finnisch, Französisch, Griechisch, Italienisch, Katalanisch, Lettisch, Litauisch, Niederländisch, Norwegisch, Polnisch, Portugiesisch, Russisch, Schwedisch, Serbokroatisch, Slowakisch, Slowenisch, Spanisch, Deutsch (Telekom), Tschechisch, Türkisch, Ungarisch, Englisch (US), Serbisch, Bulgarisch, Rumänisch und Mazedonisch.

Die grundsätzliche Spracheinstellung wird beim Systemhochlauf durch die Länderinitialisierung vorgenommen.

Verwandte Themen

- Wie Sie IP- und SIP-Teilnehmer konfigurieren
- Konfiguration der Teilnehmer

24.1.6 Flexible Menüs

Flexible Menüs ermöglichen die kundenindividuelle Anpassung der Menüpunkte im Display der Systemtelefone.

Als Administrator können Sie die Menüpunkte einzeln aus- oder einblenden.

24.1.6.1 Wie Sie das flexible Menü ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Klicken Sie im Menübaum auf **Grundeinstellungen > System > Flexible Menüs**.

4) Bearbeiten Sie die **Ausblendliste** wie folgt:

- Um einen Menüpunkt auszublenden, aktivieren Sie dessen Kontrollkästchen.
- Um einen Menüpunkt einzublenden, deaktivieren Sie dessen Kontrollkästchen.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.1.7 Wartemusik

Das Kommunikationssystem kann wartenden Teilnehmern während Vermittlungsvorgängen Wartemusik (Music On Hold, MOH) einspielen. Anrufer hören die Wartemusik, während sie gehalten, geparkt oder übergeben werden. Dies gilt auch für Anrufer in der Warteschlange der Anrufverteilung.

Das System kann Wartemusik aus folgenden Quellen einspielen:

- Interne Wartemusik
- Xpressions Compact (IVM)
  Siehe Dokumentation von Xpressions Compact. Für die Konfiguration siehe IVM in Dokumentation von Manager E.
- EXMR
  Siehe Installation OpenScape Business X1, Service Dokumentation oder Installation OpenScape Business X3/X5/X8, Service Dokumentation.
- MUSIC Einsteckmodul
  Siehe Installation OpenScape Business X1, Service Dokumentation oder Installation OpenScape Business X3/X5/X8, Service Dokumentation..
- Baugruppe MPPI-USB EXM Modul (nur für OpenScape Business X3/X5)
  Siehe Installation OpenScape Business X3/X5/X8, Service Dokumentation.

Audio-Dateien

Der Administrator kann Audio-Dateien für die interne Wartemusik vom PC in das Kommunikationssystem übertragen als alternative interne Wartemusik.

> ***INFO:*** Stellen Sie vor der Benutzung von Ansagen bzw. Musik aus anderer Quelle sicher, dass Sie keine Copyright-Verletzung begehen.

Die Audio-Dateien müssen als `Wave`-Dateien vorliegen mit folgenden Eigenschaften:

- 16 bit PCM
- Mono oder Stereo
- mögliche Abtastraten: 8 / 22,05/ 24 / 32 / 40 / 44,1 oder 48 kHz.
- Länge des Audio-Dateinamens maximal 30 Zeichen

Empfohlen: **16 bit PCM - Mono - 8 kHz, Länge ca. 2 min**

Interne Wartemusik

Für Tag - und Nachtbetrieb (Nachtschaltung) kann unterschiedliche Wartemusik konfiguriert werden.

Der Administrator kann folgende Funktionen konfigurieren:

- Wartemusik mit Rufton (Freiton):
  Der gehaltene Teilnehmer hört während der Rückfrage zunächst die Wartemusik. Nach Übergeben des gehaltenen Teilnehmers an das Ziel ertönt an Stelle der Wartemusik der Rufton.

- Wartemusik ohne Rufton (Freiton):
  Der gehaltene Teilnehmer hört die Wartemusik, bis der gerufene Teilnehmer den Anruf annimmt.
- Keine Wartemusik:
  Der gehaltene Teilnehmer hört nichts (Stille). Wird ein externes Gespräch durch Übergabe vor Melden übergeben, hört der Anrufer den Freiton.

24.1.7.1 Wie Sie interne Wartemusik importieren

Mit dem Wizard **Wartemusik / Ansagen** können Sie Audiodateien als interne Wartemusik in das Kommunikationssystem importieren.

Voraussetzungen

- Sie sind am WBM angemeldet.
- Die einzuspielenden Audio-Dateien liegen als WAVE-Dateien im geforderten Format vor.

> ***INFO:*** Stellen Sie vor der Benutzung sicher, dass Sie keine Copyright-Verletzung begehen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Zentrale Telefonie**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Wartemusik / Ansagen** zu starten.

4) Klicken Sie für Tagbetrieb bei **Wartemusik-Datei - Tag** und/oder für Nachtbetrieb bei **Wartemusik-Datei - Nacht** auf **Durchsuchen**.

5) Wählen Sie eine Audio-Datei aus und klicken Sie auf **Öffnen**. Der Pfad zur gewählten Audio-Datei wird bei **Wartemusik-Datei - Tag** und/oder **Wartemusik-Datei - Nacht** angezeigt.

6) Klicken Sie auf **Laden**.

7) Bestätigen Sie den Hinweis mit **OK** und klicken Sie auf **OK & Weiter**.

8) Klicken Sie auf **Beenden**.

9) Führen Sie wie gefordert einen Neustart des Kommunikationssystems durch über **Service-Center > Restart / Reload > System neu starten**.

24.1.7.2 Wie Sie die Funktion der internen Wartemusik konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.
- Die Länge des Wartemusik-Dateinamens beträgt maximal 30 Zeichen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Anschaltung**.

3) Klicken Sie im Menübaum auf **Anschaltungen > Ansage / Interne Wartemusik**.

4) Wählen Sie im Bereich **Interne Wartemusik** in der Aufklappliste **MOH Typ** den Eintrag **Kein Music On Hold**, **MOH ohne Rufton** oder **MOH mit Rufton**.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.1.8 Ansagen

Das Kommunikationssystem ermöglicht das Abspielen von Ansagen an Anrufer sowohl vor dem Melden, als auch bei der Nutzung der Anrufverteilung sowie bei MFV-Durchwahl. Darüber hinaus kann in bestimmten Situationen die Wartemusik durch eine Ansage ersetzt werden, z. B. bei Halten oder während ein Teilnehmer belegt ist oder vermittelt wird.

Das System kann Ansagen aus folgenden Quellen einspielen:

- Interne Ansagen
- Announcement Player (nur mit UC Booster Funktionalität)
  Der Announcement Player ist eine interne Software, die zusammen mit der UC Booster Funktionalität (UC Booster Card oder UC Booster Server) zur Verfügung steht. Wird ein Teilnehmer angerufen, spielt der Announcement Player zuerst die gewünschte Ansage vor und stellt anschließend die Verbindung zum Teilnehmer her. Für die Einrichtung wird der Manager E benötigt.
- Analoges Ansagegerät
  Siehe OpenScape Business Administratordokumentation, Kapitel Anschaltungen - Analoges Ansagegerät.
- Baugruppe MPPI-USB EXM Modul (nur für OpenScape Business X3/X5)
  Siehe Installation OpenScape Business X3/X5/X8, Service Dokumentation.

Der Administrator kann Ansagen für einmalige oder für endlos wiederholte Wiedergabe konfigurieren.

Ein externes Ansagegerät muss sich wie ein Teilnehmer verhalten, d. h. sich melden, die Ansage einspielen und das Gespräch vermitteln (in Rückfrage gehen, wählen und auflegen).

Audio-Dateien

Der Administrator kann Audio-Dateien mit Ansagen vom PC in das Kommunikationssystem übertragen.

> ***INFO:*** Stellen Sie vor der Benutzung von Ansagen bzw. Musik aus anderer Quelle sicher, dass Sie keine Copyright-Verletzung begehen.

Die Audio-Dateien müssen als `Wave`-Dateien vorliegen mit folgenden Eigenschaften:

- 16 bit PCM
- Mono oder Stereo
- mögliche Abtastraten: 8 / 22,05/ 24 / 32 / 40 / 44,1 oder 48 kHz.
- Länge des Audio-Dateinamens maximal 30 Zeichen

Empfohlen: **16 bit PCM - Mono - 8 kHz, Länge ca. 2 min**

24.1.8.1 Wie Sie Ansagen konfigurieren (UC Smart)

Die Konfiguration erfolgt in Manager E nach folgendem grundsätzlichen Ablauf (siehe auch Online-Hilfe zu Manager E):

Schritt für Schritt

1) Für den gewünschten Port der Sprachbox (UC Smart) unter **Anlagensicht**, Menü **Einstellungen > Station einrichten > Teilnehmer** den **Typ** auf **Standard** setzen. Es wird empfohlen dafür die letzten Ports zu verwenden.
2) Den gewünschten Port aus dem Sammelanschluss der Sprachbox (UC Smart) entfernen unter **Anlagensicht**, Menü **Einstellungen > Kommende Rufe > Gruppen-/Sammelanschluß**.
3) Der Rufnummer des betreffenden Ports eine Sprachbox zuweisen unter **Anlagensicht**, Menü **Einstellungen > Anschaltungen > EVM**.
4) Begrüßung auswählen und Ansage importieren unter **Maintenance > Ansage > Ansageeinrichtungen**.
5) Einmalige oder wiederholte Wiedergabe auswählen unter **Anlagensicht**, Menü **Einstellungen > Anschaltungen > Ansage**, Bereich **Ansageeinrichtungen**.

24.1.8.2 Wie Sie Ansagen konfigurieren (UC Suite)

Mit dem Wizard **Wartemusik / Ansagen** können Sie Audiodateien in das Kommunikationssystem übertragen und als Ansagen konfigurieren.

Voraussetzungen

- Sie sind am WBM angemeldet.
- Einzuspielende Audiodateien liegen als PCM-Dateien mit folgenden Eigenschaften vor: 8 kHz, 16 bit, mono. Die Länge des Audio-Dateinamens beträgt maximal 30 Zeichen.

INFO: Stellen Sie vor der Benutzung sicher, dass Sie keine Copyright-Verletzung begehen.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Zentrale Telefonie**.

3) Klicken Sie auf **Bearbeiten** um den Wizard **Wartemusik / Ansagen** zu starten.

4) Überspringen Sie die Auswahl der Wartemusik-Dateien und klicken Sie auf **OK & Weiter**.

5) Um eine Audio-Datei in das Kommunikationssystem zu übertragen:

a) Klicken Sie auf **Durchsuchen**.

b) Wählen Sie eine Audio-Datei aus.

c) Klicken Sie auf **Öffnen**.

d) Klicken Sie auf **Laden**.

e) Bestätigen Sie den Hinweis mit **OK**.

f) Wenn Sie weitere Audio-Dateien in das System übertragen wollen, wiederholen Sie diese Schritte.

6) Klicken Sie auf **OK & Weiter**.

7) Wählen Sie in der Aufklappliste **WAV-Datei** eine Ansage.

8) Wählen Sie in der Aufklappliste **Modus** die Art der Wiedergabe.

9) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

24.1.8.3 Wie Sie den Announcement Player konfigurieren (nur mit UC Booster)

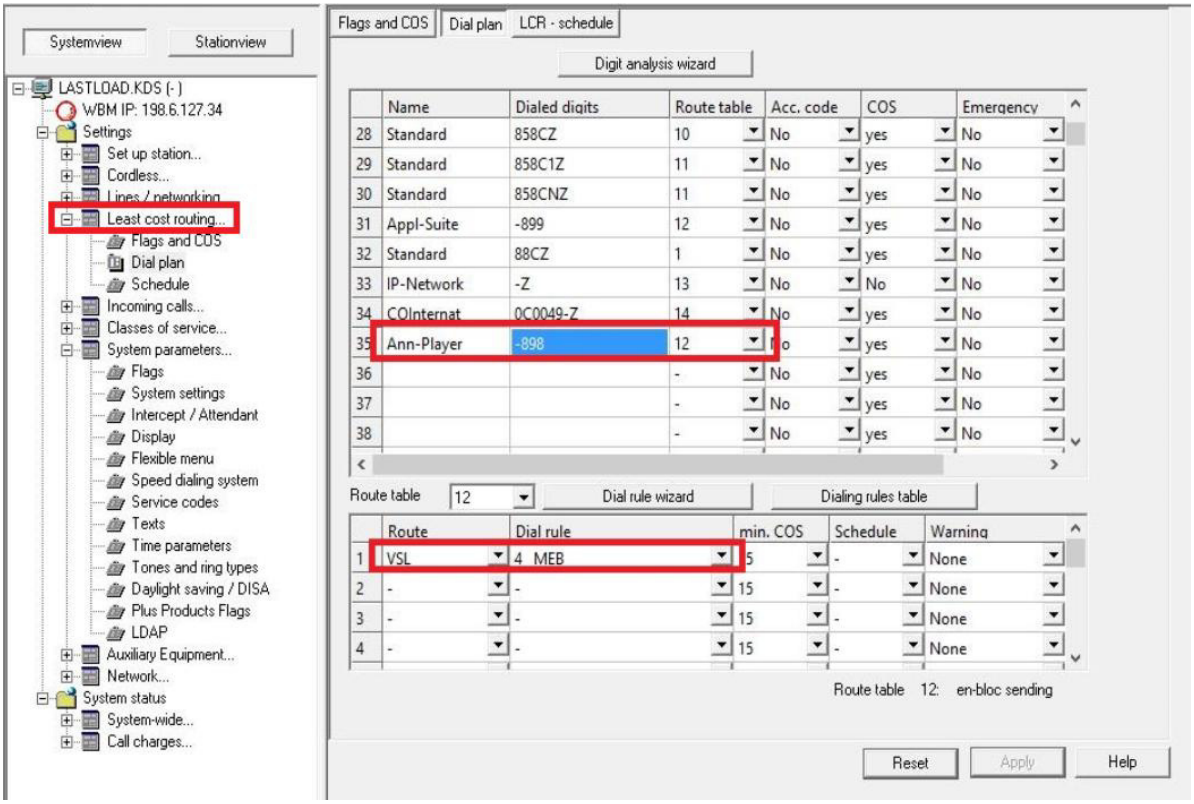
Voraussetzungen

- Der Manager E ist gestartet.
- Einzuspielende Audiodateien liegen als PCM-Dateien mit folgenden Eigenschaften vor: 8 kHz, 16 bit, mono. Die Länge des Audio-Dateinamens beträgt maximal 30 Zeichen.

INFO: Stellen Sie vor der Benutzung sicher, dass Sie keine Copyright-Verletzung begehen.

Schritt für Schritt

1) Laden Sie den KDS des Kommunikationssystems in den Manager E (siehe *Wie Sie den KDS in den Manager E laden*).
2) Klicken Sie in der Anlagenansicht auf **Einstellungen > Systemparameter**.
3) Klicken Sie auf die Registerkarte **Systemeinstellungen**.
4) Klicken Sie im Bereich **Zugangsnummer Ansagewiedergabegerät** auf **Zugangsnr. für Wiedergabegerät festlegen**.
5) Wählen Sie unter **Richtung** den Eintrag **UC Suite** oder **VSL** aus und geben Sie unter **Ruf-Nr.** die Rufnummer für den Announcement Player ein (z. B. `898`). Diese Rufnummer muss anschließend bei der Rufweiterschaltung angegeben werden. Bestätigen Sie abschließend mit **OK**.
6) Klicken Sie auf **Übernehmen**.
7) Klicken Sie in der Anlagenansicht auf **Einstellungen > Automatische Wegesuche**.
8) Klicken Sie auf die Registerkarte **Wahlplan**.
9) Kontrollieren Sie den Listen-Eintrag **Ann-Player**:



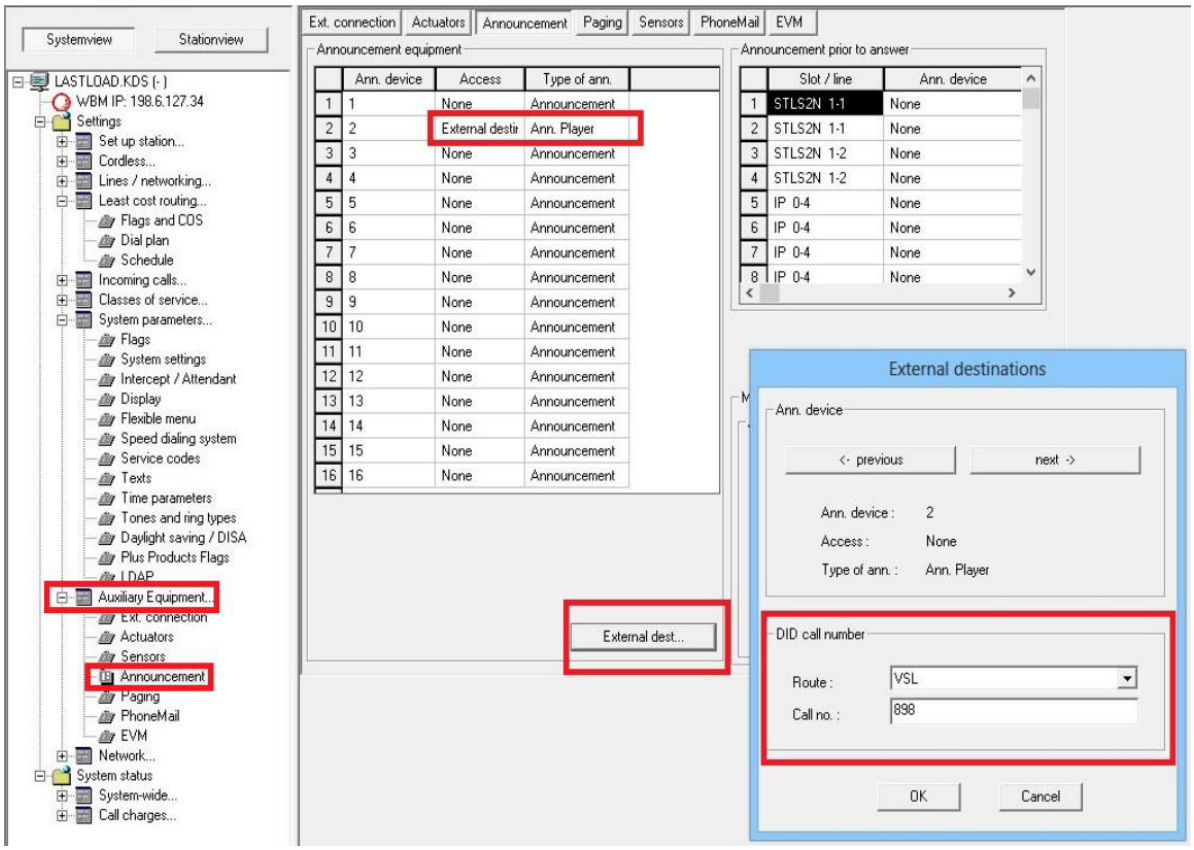
a) Bei dem Namen **Ann-Player** muss unter **Gewählte Ziffern** ein Minuszeichen gefolgt von der zuvor eingegebenen Rufnummer eingetragen sein (z. B. `-898`).

b) Die zugehörige **Wegetabelle** muss auf `12` stehen mit den Einträgen **UC Suite** oder **VSL** bei **Richtung** und **MEB** bei **Wahlregel**.

10) Klicken Sie in der Anlagenansicht auf **Einstellungen > Anschaltungen**.

11) Klicken Sie auf die Registerkarte **Ansage**.

12) Setzen Sie den Announcement Player als externes Ziel:



a) Wählen Sie in einem Listeneintrag ab Zeile 2 (Zeile 1 darf nicht geändert werden - sie wird für die interne Wartemusik genutzt) unter **Access** den Eintrag **Externes Ziel** aus und unter **Ansageart** den Eintrag **Wiedergabegerät**.

b) Wenn Sie weitere Ansagen einrichten wollen, wiederholen Sie den vorherigen Schritt und bearbeiten weitere Listeneinträge.

c) Klicken Sie auf die Schaltfläche **Externe Ziele**.

d) Wählen Sie unter **Richtung** den Eintrag **UC Suite** aus und geben Sie unter **Ruf-Nr.** die Rufnummer für den Announcement Player ein (z. B. `898`). Bestätigen Sie abschließend mit **OK**.

13) Klicken Sie auf **Übernehmen**.

14) Sichern Sie den KDS zurück in das Kommunikationssystem (siehe).

15) Melden Sie sich am WBM mit dem Profil **Expert** an (siehe).

16) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

17) Klicken Sie im Navigationsbaum auf **Wizards > Zentrale Telefonie**.

18) Klicken Sie auf **Bearbeiten** um den Wizard **Wartemusik / Ansagen** zu starten.

19) Überspringen Sie die Auswahl der Wartemusik-Dateien und klicken Sie auf **OK & Weiter**.

20) Um eine Audio-Datei in das Kommunikationssystem zu übertragen:

- ***a)*** Klicken Sie auf **Durchsuchen**.
- ***b)*** Wählen Sie eine Audio-Datei aus.
- ***c)*** Klicken Sie auf **Öffnen**.
- ***d)*** Klicken Sie auf **Laden**.
- ***e)*** Bestätigen Sie den Hinweis mit **OK**.
- ***f)*** Wenn Sie weitere Audio-Dateien in das System übertragen wollen, wiederholen Sie diese Schritte.

21) Klicken Sie auf **OK & Weiter**.

22) Wählen Sie bei dem Zugang **Externes Ziel** in der Aufklappliste **WAV-Datei** eine Ansage und wählen Sie in der Aufklappliste **Modus** die Art der Wiedergabe.

23) Wenn Sie weitere Ansagen einrichten wollen, wiederholen Sie den vorherigen Schritt.

24) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

25) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

26) Klicken Sie im Navigationsbaum auf **Middleware**.

27) Navigieren Sie im Menübaum auf **Middleware > Wiedergabegerät für Ansagen**.

28) Klicken Sie auf die Registerkarte **Einstellungen - Wiedergabegerät für Ansagen**.

29) Aktivieren Sie das Kontrollkästchen **Dienst wird automatisch gestartet**.

30) Klicken Sie auf **Übernehmen**.

31) Klicken Sie im Navigationsbaum auf **Telefonie > Kommende Rufe**.

32) Navigieren Sie im Menübaum zu **Kommende Rufe > Rufweiterschaltungen**.

33) Klicken Sie auf die Registerkarte **Rufzielliste - Definition**.

34) Wählen Sie eine freie Rufzielliste (z. B. Rufzielliste 1).

35) Wählen Sie unter **1. Ziel** eine der konfigurierten Ansagen aus (z. B. `#802 Ans`). Das Anzeigen aller Einträge kann u. U. einige Zeit dauern.

36) Wählen Sie unter **2. Ziel** den Eintrag **Angewählter Teilnehmer** aus.

37) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

38) Klicken Sie auf die Registerkarte **Rufzielliste - Zuordnung**.

39) Wählen Sie in der Zeile des gewünschten Teilnehmers in den Aufklapplisten **Tag**, **Nacht** und **Intern** die zuvor definierte Rufzielliste (z. B. Rufzielliste 1) aus.

40) Wiederholen Sie den vorherigen Schritt für weitere Teilnehmer.

Wird ein Teilnehmer angerufen, dem die Rufzielliste 1 zugeordnet ist, spielt der Announcement Player zuerst die eingerichtete Ansage vor und stellt anschließend die Verbindung zum Teilnehmer her.

41) Klicken Sie auf **Übernehmen**.

24.1.9 Teilnehmer-zu-Teilnehmer Zeichengabe

Das Kommunikationssystem ermöglicht die transparente Übertragung von Nachrichten zwischen Endgeräten (User to User Signalling, UUS). Unterstützt wird die Variante UUS1 für den Austausch von Informationen in Steuernachrichten des Verbindungsauf- und Abbaus.

Bei einem Mehrgeräte-Anschluss ist zu gewährleisten, dass maximal ein Endgerät auf einen ankommenden Ruf eine Nachricht übermittelt.

24.1.10 Sprachkanal-Signalisierungsschutz

Das Kommunikationssystem bietet einen durch den Administrator einrichtbaren Schutz vor Datenverfälschung durch unerwünschte Toneinblendungen in den Sprachkanal. Aufschalten auf eine so geschützte Verbindung ist nicht möglich. Jeder als Fax konfigurierte Teilnehmer hat diesen Signalisierungsschutz automatisch.

Wiederanrufe werden bis zum Freiwerden der Nebenstelle zurückgestellt.

Ein gehaltener Teilnehmer hat immer Signalisierungsschutz.

24.1.11 Zeitparameter

Das Kommunikationssystem bietet dem Administrator Einstellmöglichkeiten für diverse Zeitparameter, wie z. B. für die Dauer des Rückrufes oder die Zeit für automatische Wahlwiederholung.

Die Zeitparameter sind im Kommunikationssystem voreingestellt und müssen in der Regel nicht verändert werden.

24.1.12 Steuerung von Centrex-Leistungsmerkmalen

Zur Steuerung von Centrex-Leistungsmerkmalen müssen die Wählzeichen * und # ins ISDN und zu ITSP übertragen werden.

Als Administrator können Sie dieses Leistungsmerkaml aktivieren oder deaktivieren.

Die Eingabe einer Kennzahl muss im Wahlzustand erfolgen (zum Beispiel nach Eingabe der Leitungskennzahl). Die Eingabe beginnt immer mit * oder #, gefolgt von einer Ziffer oder Ziffernkombination und endet mit #.

24.1.12.1 Wie Sie die Steuerung von Centrex-Leistungsmerkmalen aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Grundeinstellungen**.

3) Navigieren Sie im Menübaum zu **System > System Flags**.

4) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie die Steuerung von Centrex-Leistungsmerkmalen aktivieren möchten, aktivieren Sie das Kontrollkästchen **Wahl von * und # auf Leitungsschnittstellen**.
- Wenn Sie die Steuerung von Centrex-Leistungsmerkmalen deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Wahl von * und # auf Leitungsschnittstellen**.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.2 Sichern und Wiederherstellen

Die Konfigurationsdaten des Kommunikationssystems können gesichert und wiederhergestellt werden.

Die Konfigurationsdaten werden in einem Backup-Set abgespeichert. Jede Sicherung erzeugt ein eigenes Backup-Set. Die Sicherung kann sofort manuell oder automatisch zu bestimmten Zeitpunkten durchgeführt werden.

INFO: Es wird dringend empfohlen, die Konfigurationsdaten regelmäßig als Backup-Sets zu sichern.

Bei einem Update auf ein neues Minor Release ist es erforderlich, ein neues Backup-Set zu erstellen.

Es kann auf unterschiedliche Backup-Medien gesichert werden (wie z. B. auf ein USB-Medium, ein Netzlaufwerk oder die Festplatte der UC Booster Card).

Abhängig von der Systemkonfiguration, der Nutzung des Kommunikationssystems und der Art des Backup-Mediums kann eine Sicherung oder Wiederherstellung eine längere Zeit in Anspruch nehmen - bei Systemen mit UC Suite im

Einzelfall bis zu drei Stunden. Dieser Vorgang sollte nicht manuell oder durch einen System-Neustart abgebrochen werden.

Der Abbruch einer Datenwiederherstellung kann zu einer inkonsistenten Systemkonfiguration führen, in der ein fehlerfreier Betrieb des Systems nicht gewährleistet ist. Eine abgebrochene Wiederherstellung sollte unbedingt wiederholt werden, bis diese erfolgreich abgeschlossen ist. Andernfalls kann eine vollständige Neueinrichtung des Systems erforderlich werden. Falls die Wiederherstellung mehrfach fehlschlägt, verständigen Sie bitte den Service-Support und stellen Sie zwischenzeitlich sicher, dass ihre Datensicherung nicht durch neue Backups überschrieben wird. Dazu muss die automatische Datensicherung vorübergehend deaktiviert werden.

Backup-Sets für Diagnosezwecke

Für Diagnosezwecke können "kleinere" Backup-Sets erzeugt werden, die Daten für die Fehlersuche durch den Service-Support enthalten. Im Gegensatz zu den normalen Backup-Sets werden wesentlich kleinere Datenmengen erzeugt und damit zum Beispiel ein einfaches Versenden per E-Mail ermöglicht. Diagnose-Backup-Sets enthalten unter anderem die Konfigurationsdaten des Kommunikationssystems und der installierten UC-Lösung. Sprachnachrichten, Faxnachrichten und Ansagen sind nicht enthalten.

Backup-Verzeichnis "Hard disk" (nur bei UC Booster Card)

Ist die UC Booster Card gesteckt, können die Konfigurationsdaten des Kommunikationssystems in einer eigenen Partition der Festplatte der UC Booster Card im Backup-Verzeichnis gespeichert werden. Dieses Backup-Verzeichnis ist als Standard-Archiv "Hard disk" bereits vorgeleistet.

Sicherung der Konfigurationsdaten des UC Booster Servers

Wird zusätzlich zum Kommunikationssystem ein UC Booster Server betrieben, so sollte bei einer Sicherung der Konfigurationsdaten des Systems auch die Konfigurationsdaten des UC Booster Servers gesichert werden. Der Sicherung der Daten des UC Booster Servers erfolgt identisch zum Sicherung der Daten des Kommunikationssystems, nur dass der Administrator beim Aufruf des WBM nicht die IP-Adresse des Kommunikationssystems angibt, sondern die IP-Adresse des Linux-Servers.

24.2.1 Backup-Sets

Die Konfigurationsdaten des Kommunikationssystems werden in einem Backup-Set gesichert.

Zusätzlich zum Backup-Set ist eine zu dem Backup-Set gehörige Text-Datei zu speichern. Sie enthält Informationen über Datum und Uhrzeit der Sicherung und unter welcher Software-Version die Sicherung durchgeführt wurde. Die Text-Datei ist notwendig für die Wiederherstellung des Backup-Sets.

Übersteigt die Anzahl der gespeicherten Backup-Sets den eingestellten Wert, so werden die ältesten Backup-Sets gelöscht.

Backup-Set-Daten

Folgende Daten zu einem Backup-Set werden angezeigt:

- **Archivname**: Name des Backup-Sets.
- **Grösse**: Größe des Backup-Sets in Bytes.
- **Datum**: Datum, an dem das Backup-Set erstellt wurde.
- **Kommentar**: Kommentar, der bei der Erstellung des Backup-Sets mit angegeben wurde (optional).

Ausgegraut dargestellte Backup-Sets können nicht wiederhergestellt werden.

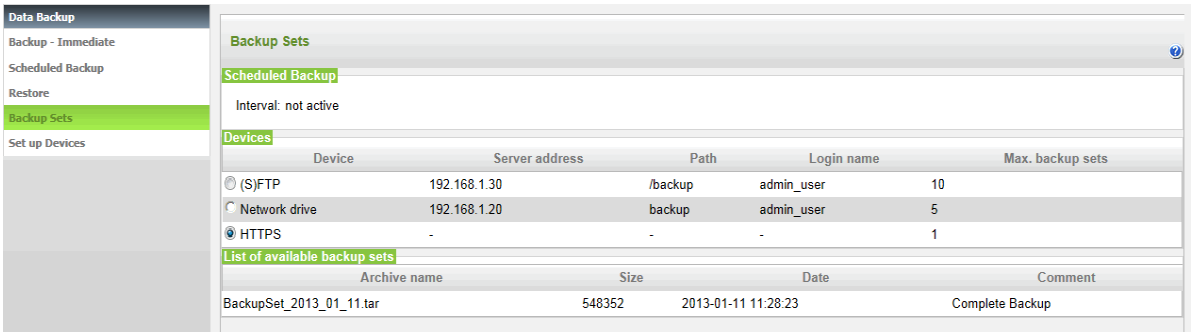
24.2.1.1 Wie Sie sich Backup-Sets anzeigen lassen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Datensicherung**.
2) Klicken Sie im Navigationsbaum auf **Backup Sets**.
3) Aktivieren Sie im Bereich **Geräte** das Backup-Medium, dessen Backup-Sets Sie sich anzeigen lassen wollen. Sie erhalten eine Liste aller auf diesem Medium verfügbaren Backup-Sets.



24.2.1.2 Wie Sie Backup-Sets löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Datensicherung**.
2) Klicken Sie im Navigationsbaum auf **Backup Sets**.

3) Aktivieren Sie im Bereich **Geräte** das Backup-Medium, dessen Backup-Sets Sie sich anzeigen lassen wollen. Sie erhalten eine Liste aller auf diesem Medium verfügbaren Backup-Sets.

4) Aktivieren Sie das Kontrollkästchen des Backup-Sets, das Sie löschen wollen und klicken Sie auf **Löschen**. Das Backup-Set wird gelöscht.

24.2.2 Backup-Medien

Auf den Backup-Medien werden die Backup-Sets gesichert.

Für die Sicherung können folgende Backup-Medien verwendet werden:

- Gestecktes USB-Medium
- Netzlaufwerk
- Client-PC über HTTPS (nur möglich bei sofortiger Sicherung)
- Festplatte der UC Booster Card
- FTP-/FTPS-Server

Für jedes Backup-Medium kann festgelegt werden, wieviele Backup-Sets maximal in dem Verzeichnis abgelegt werden dürfen.

USB-Medium

Um ein USB-Medium (z. B. USB-Festplatte oder USB-Stick) für das Backup zu verwenden, muss das USB-Medium an der USB-Server-Schnittstelle des Kommunikationssystems gesteckt sein, damit es für die Sicherung zur Verfügung steht. Zusätzlich muss das USB-Medium mit FAT-32 formatiert sein. Vom einem NTFS formatierten USB-Medium kann nur gelesen werden. Sind mehrere Partitionen vorhanden, ist eine Sicherung nur auf der ersten Partition möglich!

Ein bootfähiges USB-Medium wird nicht unterstützt.

Bei OpenScape Business S und OpenScape UC Booster Server wird das USB-Medium in die USB-Schnittstelle des Linux-Servers gesteckt.

FTP-/FTPS-Server und Netzlaufwerke

FTP-/FTPS-Server und Netzlaufwerke können als neue Medien hinzugefügt, bearbeitet oder gelöscht werden. FTP-/FTPS-Server und Netzlaufwerke können auch mehrfach angegeben werden, wenn dabei unterschiedliche Verzeichnisse genutzt werden. Als verschlüsseltes File-Transfer-Protokoll (FTPS) wird SSL/TLS unterstützt.

Der Benutzer muss für die Sicherung der Konfigurationsdaten auf einem FTP-/FTPS-Server Schreibrechte für sein Root-Verzeichnis haben. Für die Sicherung auf einem Netzlaufwerk reichen Schreibrechte für das gewünschte Verzeichnis.

Ist die Übertragungsgeschwindigkeit zum FTPS-Server zu niedrig, kann es zu einer Fehlfunktion bei der Datensicherung kommen. In diesem Fall muss die Datensicherung neu gestartet werden.

Bei FTPS werden Zertifikate bis 2048 Bit unterstützt. Diese Zertifikate sind für die Authentifizierung am FTPS-Server nötig.

24.2.2.1 Wie Sie ein Backup-Medium hinzufügen

Voraussetzungen

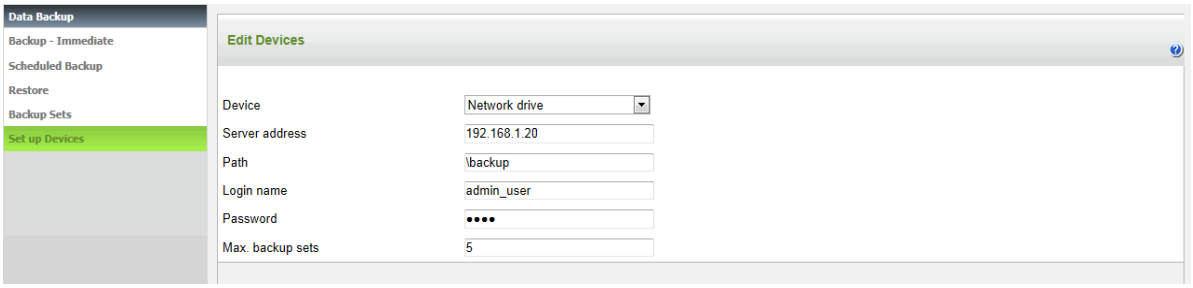
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Datensicherung**.

2) Klicken Sie im Navigationsbaum auf **Einrichtung Geräte**.

3) Klicken Sie auf **Hinzufügen**.



4) Wählen Sie in der Aufklappliste in der Spalte **Gerät** das gewünschte Backup-Medium aus:

- Wenn Sie auf einem FTP-/FTPS-Server sichern wollen, wählen Sie **(S)FTP** aus.
- Wenn Sie auf einem Netzlaufwerk sichern wollen, wählen Sie **Network drive** aus.

5) Geben Sie unter **Server-Adresse** den Hostnamen oder die IP-Adresse des Mediums ein.

6) Geben Sie unter **Verzeichnis** den Pfad an, in dem das Backup-Set gespeichert werden soll.

7) Wenn Sie auf einem FTP-/FTPS-Server sichern wollen, geben Sie **Benutzername** und **Passwort** für den Zugang zum FTP-/FTPS-Server ein.

8) Wenn Sie auf einem Netzlaufwerk sichern wollen, das gesichert ist, geben Sie **Benutzername** und **Passwort** für den Zugang zum Netzlaufwerk ein.

9) Geben Sie unter **Max. Backup-Sets** die Anzahl der Backup-Sets ein, die maximal in dem Verzeichnis gespeichert werden sollen.

10) Klicken Sie auf **OK & Weiter**. Das neu angelegte Backup-Medium erscheint in der Liste der verfügbaren Backup-Medien.

11) Klicken Sie im Navigationsbaum auf **Backup Sets**.

12) Aktivieren Sie im Bereich **Geräte** das Backup-Medium, das Sie gerade hinzugefügt haben. Ist in der Liste der verfügbaren Backup-Sets kein roter Balken mit einer Fehlermeldung zu sehen, ist das Backup-Medium korrekt eingerichtet.

13) Wird eine Fehlermeldung angezeigt, überprüfen Sie nochmals Ihre Eingaben (siehe *Wie Sie ein Backup-Medium bearbeiten*

24.2.2.2 Wie Sie ein Backup-Medium bearbeiten

Voraussetzungen

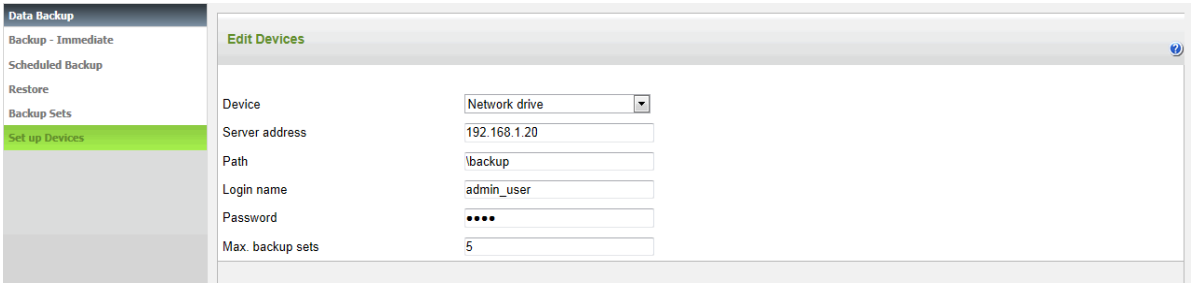
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Datensicherung**.

2) Klicken Sie im Navigationsbaum auf **Einrichtung Geräte**.

3) Aktivieren Sie das zu bearbeitende Backup-Medium und klicken Sie auf **Bearbeiten**.



4) Ändern Sie die gewünschten Werte.

5) Klicken Sie auf **OK & Weiter**.

24.2.2.3 Wie Sie ein Backup-Medium löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Datensicherung**.

2) Klicken Sie im Navigationsbaum auf **Einrichtung Geräte**.

3) Wählen Sie das zu löschende Backup-Medium aus und klicken Sie auf **Löschen**.

Es können auch mehrere Backup-Medien zum Löschen ausgewählt werden.

4) Bestätigen Sie die Sicherheitsabfrage mit **OK**. Das Backup-Medium ist aus der Liste der verfügbaren Backup-Medien gelöscht.

24.2.3 Sofortiges Sichern

Die Konfigurationsdaten können manuell sofort gesichert werden.

Die Sicherung kann auf unterschiedlichen Backup-Medien erfolgen. Standardmäßig ist das Backup-Medium **HTTPS** eingerichtet. Damit können Sie das Backup-Set an allen Speicherorten ablegen, auf die der Client-PC Zugriff hat, mit dem Sie sich am WBM angemeldet haben. Der gewählte Speicherort muss auch bei der Wiederherstellung des Backup-Sets zugänglich sein. Ist ein USB-Medium am Kommunikationssystem angeschlossen, wird als zusätzliches Backup-Medium **USB-Device** angezeigt. Ist die UC Booster Card inkl. Festplatte gesteckt, wird ein weiteres Backup-Medium **Hard disk** angezeigt.

Der Name des Backup-Sets wird bei der Sicherung automatisch vergeben. Er beinhaltet u.a. das Datum, an dem die Sicherung durchgeführt wird. Zusätzlich sind diese Daten auch in einer Text-Datei enthalten, die zusätzlich abgespeichert werden muss. Um das Backup-Set bei einer möglichen Wiederherstellung leichter identifizieren zu können, kann ein Kommentar angegeben werden.

24.2.3.1 Wie Sie ein Backup-Set sofort sichern

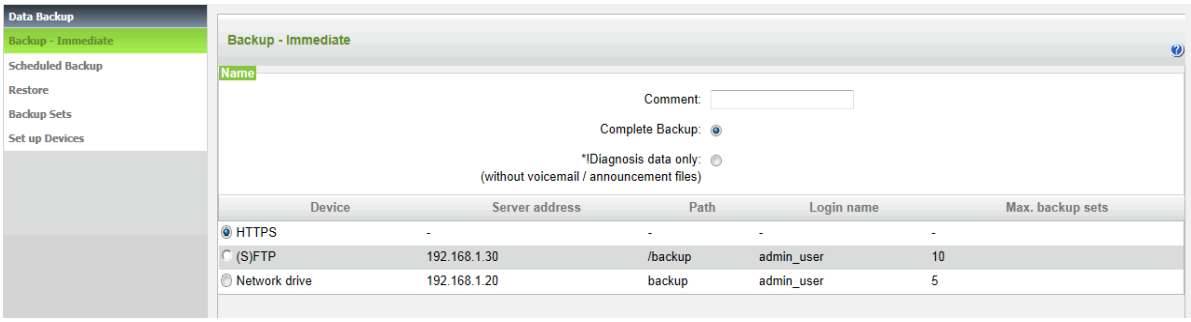
Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.
- Nur bei Nutzung von UC Suite: UC Suite ist korrekt gestartet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Datensicherung**.

2) Klicken Sie im Navigationsbaum auf **Backup - sofort**.



3) Geben Sie im Feld **Kommentar** einen Kommentar für das Backup-Set ein, um das Backup-Set bei einer möglichen Wiederherstellung leichter identifizieren zu können. Vermeiden Sie bei der Eingabe Umlaute und Sonderzeichen.

4) Wenn Sie ein Backup-Set inkl. Sprachnachrichten und Ansagen erstellen wollen, aktivieren Sie die Option **Vollständiges Backup**.

5) Wenn Sie ein Backup-Set ohne Sprachnachrichten und Ansagen erstellen wollen, aktivieren Sie die Option **Nur Diagnose-Daten**.

6) Aktivieren Sie im Bereich **Geräte** das Ziellaufwerk, auf dem das Backup-Set gespeichert werden soll.

7) Klicken Sie auf **OK & Weiter**. In einem weiteren Fenster wird Ihnen der Fortschritt der Sicherung angezeigt.

> ***INFO:*** Falls die Schaltfläche **OK & Weiter** ausgegraut ist, sind nicht alle Applikationen (z. B. UC Suite) korrekt gestartet, deren Daten gesichert werden sollen.
>
> Falls Sie für das ausgewählte Archiv-Verzeichnis keine Berechtigung haben, erhalten Sie eine Fehlermeldung. Wählen Sie ein anderes Ziellaufwerk aus oder ändern Sie den Pfad für das Archiv.
>
> Falls auf dem Ziellaufwerk nicht genügend Speicherplatz für das Backup-Set vorhanden ist, erhalten Sie eine Fehlermeldung. Wählen Sie ein anderes Ziellaufwerk oder löschen Sie ein Backup-Set und starten Sie die Datensicherung erneut.

8) Die Sicherung ist erfolgreich, wenn die Meldung **Sicherung erfolgreich ausgeführt! 100%** erscheint.

9) Wenn Sie als Backup-Medium **HTTPS** ausgewählt haben, müssen Sie das Backup-Set und die zum Backup-Set gehörige Text-Datei an einem Speicherort Ihrer Wahl sichern. Bei den anderen Backup-Medien geschieht dies automatisch. Das Browser-Fenster muss solange geöffnet bleiben, bis der Speichervorgang für Backup-Set und Text-Datei abgeschlossen ist.

> ***INFO:*** Wenn Sie als Backup-Medium ein USB-Medium verwenden, warten Sie ab, bis die LED des USB-Mediums aufhört zu blinken. Erst dann ist die Sicherung erfolgreich auf dem USB-Medium gespeichert. Entfernen Sie anschließend das USB-Medium.

10) Klicken Sie auf **Beenden**.

24.2.4 Zeitgesteuertes Sichern

Über eine Zeitsteuerung können die Konfigurationsdaten automatisch gesichert werden. Zeitpunkt, Intervall und Ort der automatischen Sicherung ist einstellbar.

Die zeigesteuerte Datensicherung kann täglich oder wöchentlich für eine feste Uhrzeit geplant werden und startet dann automatisch. Dieser "Sicherungsauftrag" kann für ein internes oder externes Sicherungsmedium eingerichtet werden. Die Einrichtung mehrerer Sicherungsaufträge ist nicht möglich.

24.2.4.1 Wie Sie ein Backup-Set zeitgesteuert sichern

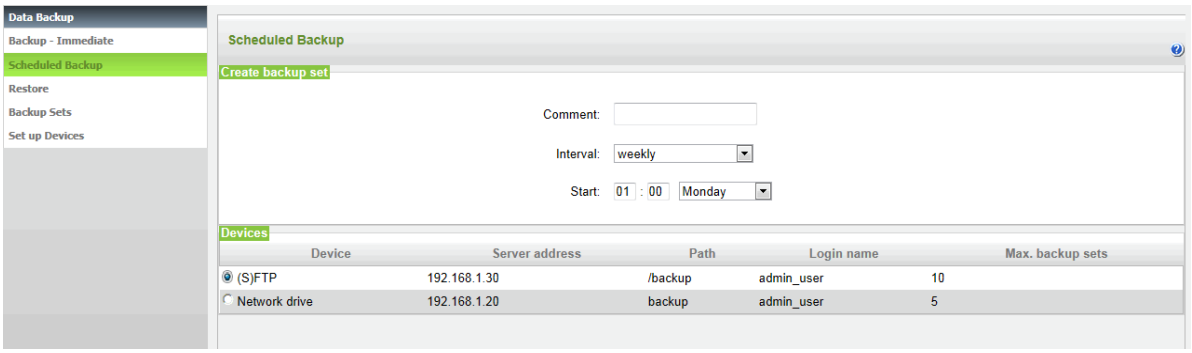
Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Datensicherung**.

2) Klicken Sie im Navigationsbaum auf **Backup - zeitgesteuert**.



3) Geben Sie im Bereich **Backup-Set erstellen** im Feld **Kommentar** einen Kommentar für das Backup-Set ein, um das Backup-Set bei einer möglichen Wiederherstellung leichter identifizieren zu können. Vermeiden Sie bei der Eingabe Umlaute und Sonderzeichen.

4) Legen Sie das Intervall für die Sicherung fest:

- tägliche Datensicherung: Wählen Sie in der Aufklappliste **Intervall** den Eintrag **täglich** und geben Sie bei **Backup - Zeitpunkt** an, wann die Datensicherung jeden Tag starten soll.
- wöchentliche Datensicherung: Wählen Sie in der Aufklappliste **Intervall** den Eintrag **wöchentlich** und geben Sie bei **Backup - Zeitpunkt** an, an welchem Wochentag und um welche Zeit die Datensicherung starten soll.

5) Aktivieren Sie im Bereich **Geräte** das Ziellaufwerk, auf dem das Backup-Set gespeichert werden soll.

6) Klicken Sie auf **OK & Weiter**. Die Datensicherung wird täglich oder wöchentlich zum angegebenen Zeitpunkt automatisch gestartet.

24.2.5 Wiederherstellen

Die Wiederherstellung der Konfigurationsdaten erfolgt manuell über die Backup-Sets.

Die Wiederherstellung kann von allen unterstützten Backup-Medien erfolgen.

24.2.5.1 Wie Sie ein Backup-Set wiederherstellen

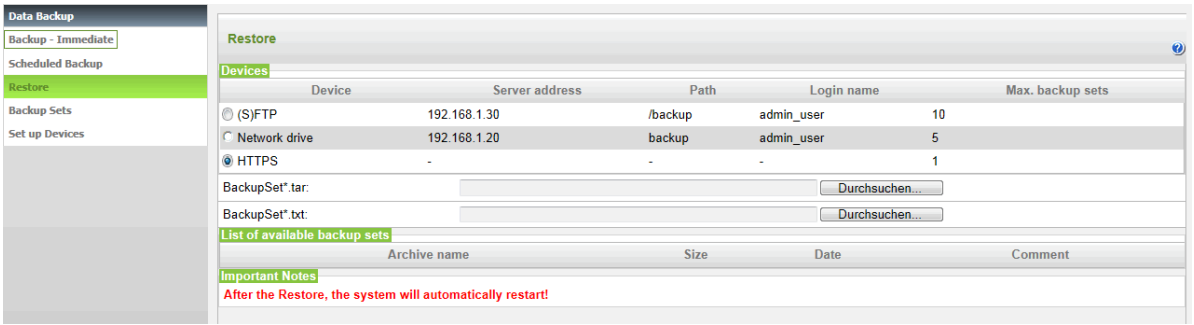
Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.
- Nur bei Nutzung von UC Suite: UC Suite ist korrekt gestartet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Datensicherung**.

2) Klicken Sie im Navigationsbaum auf **Restore**.



3) Aktivieren Sie im Bereich **Geräte** das Medium, das das wiederherzustellende Backup-Set enthält.

4) Wenn Sie als Backup-Medium **HTTPS** aktiviert haben, navigieren Sie zu dem Speicherort des Backup-Sets und wählen das Backup-Set aus. Navigieren Sie anschließend zum Speicherort der Text-Datei und wählen Sie diese aus.

5) Wenn Sie ein anderes Backup-Medium als **HTTPS** aktiviert haben, aktivieren Sie im Bereich **Liste der verfügbaren Backupsets** das Backup-Set, das die wiederherzustellenden Konfigurationsdaten enthält.

6) Warten Sie bis die Dateien auf das System geladen wurden und klicken Sie anschließend auf **OK & Weiter**. Die Wiederherstellung der Konfigurationsdaten wird gestartet. Es wird Ihnen der Fortschritt der Wiederherstellung angezeigt.

7) Nachdem die Meldung **Restore erfolgreich ausgeführt!** erscheint, führt das System automatisch ein Neustart durch. Die Wiederherstellung ist erfolgreich abgeschlossen, wenn das System wieder betriebsbereit ist.

24.3 Update

Mit Hilfe von Updates wird die Software der Systemkomponenten innerhalb einer Version aktualisiert.

Die Version der installierten Software wird auf der Startseite des WBM angezeigt. Ist eine aktuellere Software verfügbar, wird dies dort mitgeteilt.

INFO: Bei einem Update auf ein neues Minor Release ist es erforderlich, ein neues Backup-Set zu erstellen.

Die Software-Aktualisierung wird mit dem WBM durchgeführt. Bei einer Hardware-Plattform gibt es zusätzlich die Möglichkeit, die Software direkt über einen USB-Medium ohne WBM-Zugriff zu aktualisieren. Bei einem Kommunikationssystem mit UC Booster Server werden Hardware-Plattform und UC Booster Server separat aktualisiert.

Mit Hilfe des WBM kann die Software über den Internet-Webserver, einen lokalen Webserver oder direkt über Image-Dateien aktualisiert werden.

Folgende Systemkomponenten werden aktualisiert:

- Software des Kommunikationssystems
- Software der UC Clients
- Software der Systemtelefone (Aktualisierung auch einzeln möglich)
- Dokumentation

Zusammen mit der Software des Kommunikationssystems wird die Software der UC Clients aktualisiert. Liegt eine aktuellere Software vor, erhalten die Benutzer der UC Clients über das Auto-Update eine Nachricht, dass ein Update zur Verfügung steht und installiert werden kann.

Die Software-Aktualisierung der IP-Systemtelefone erfolgt automatisch zusammen mit der Aktualisierung des Kommunikationssystems, kann aber auch manuell durchgeführt werden. Für die UP0-Systemtelefone erfolgt die Aktualisierung manuell mit dem Manager E.

Die Software-Aktualisierung kann sofort gestartet werden oder die Zeitpunkte für Software-Übertragung und Software-Aktivierung können getrennt voneinander festgelegt werden. Die Aktualisierung sollte außerhalb der Kundengeschäftszeiten durchgeführt werden, da das Kommunikationssystem und/oder die Systemtelefone neu gestartet werden und bestehende Gespräche und die Nutzung der UC Clients unterbrochen werden.

Ist die Software auf das Kommunikationssystem übertragen worden, wird die Software zum gewählten Zeitpunkt aktiviert. Anschließend wird automatisch das aktuellste Telefon-Image auf die IP-Systemtelefone geladen. Nach einem Neustart des Kommunikationssystems und der IP-Systemtelefone ist die neu geladenen Software aktiv.

Image-Dateien

Für die Aktualisierung der Systemkomponenten werden Image-Dateien benötigt, die die Software der Systemkomponenten enthalten. Diese Image-Dateien können z. B. vom Software-Server (Internet-Webserver) heruntergeladen und eigenständig auf einem lokalen Webserver oder im internen Netz oder auf einem USB-Stick abgelegt werden. Es gibt eine eigene Image-Datei für das Kommunikationssystem ohne UC Booster Card und eine eigene Image-Datei für ein System mit UC Booster Card. Beide Image-Dateien enthalten auch die Software für die Systemtelefone. Zusätzlich gibt es aber auch für jeden Systemtelefontyp eine eigene Image-Datei, falls die Systemtelefone separat aktualisiert werden sollen.

Es gibt folgende Typen von Image-Dateien:

- **tgz**: für die Software des Kommunikationssystems. In der tgz-Datei befindet sich eine tar-Datei. Die tar-Datei muss mit einem Entpacker wie z. B. WinZip oder 7-zip aus der tgz-Datei entpackt werden. Die tgz-Datei wird deshalb zum Download angeboten, weil damit beim Herunterladen vom Software-Server überprüft werden kann, ob die Datei beschädigt ist oder nicht.
- **tar**: für die Software des Kommunikationssystems. Sie enthält die gepackten Dateien für die einzelnen Systemkomponenten.
- **app**: für die Software des Systemtelefons.

Lokaler Webserver

Bei der Software-Aktualisierung über einen Webserver wird standardmäßig auf den Software-Server (Internet-Webserver) zugegriffen.

Es ist aber auch möglich für die Aktualisierung einen lokalen Webserver zu verwenden. Dafür muss die Image-Datei auf dem lokalen Webserver abgelegt sein und der Pfad zum lokalen Webserver im WBM konfiguriert sein.

Speed-Upgrade

Ein Speed-Upgrade wie bei der HiPath 3000 ist nicht möglich.

WICHTIG: Ein Ziehen der SDHC-Karte während des Betriebs führt zu Datenverlust!

24.3.1 Nutzung eines lokalen Webservers

Die Software kann über einen lokalen Webserver aktualisiert werden.

Die aktuellen Image-Dateien müssen auf dem lokalen Webserver abgelegt sein. Zusätzlich sind die Zugangsdaten des lokalen Webservers im WBM einzutragen. Diese Änderung kann nur von einem Administrator mit dem Profil **Expert** durchgeführt werden. Sind die Zugangsdaten des lokalen Webservers eingetragen, werden diese als Standard gesetzt und für alle weiteren Updates des Kommunikationssystems wird jetzt anstelle des Internet-Webservers der lokale Webserver verwendet.

24.3.1.1 Wie Sie den Zugang zum lokalen Web-Server konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.
- Eine Verbindung zum lokalen Webserver ist vorhanden.
- Sie benötigen die Web-Adresse (URL) und die Zugangskennung des lokalen Webservers sowie den Namen der Image-Datei.
- Die Image-Datei ist als tar-Datei auf dem lokalen Webserver gespeichert und der Ablageort ist bekannt. Evtl. mus die tar-Datei aus der gespeicherten tgz-Datei entpackt werden.
- Wenn Sie für die Aktualisierung einen Proxy-Server verwenden, benötigen Sie noch dessen Daten (evtl. auch Benutzername und Passwort).

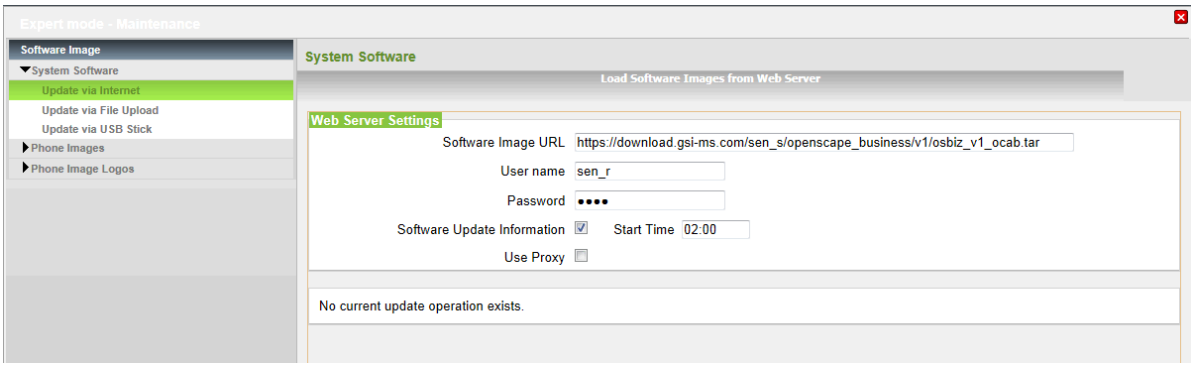
Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung > Software-Image**.

3) Klicken Sie im Menübaum auf **System Software**.

4) Klicken Sie auf **Update via Internet**.



5) Richten Sie den Zugang zum lokalen Webserver ein:

a) Geben Sie unter **Software-Image URL** die Adresse des lokalen Webservers inkl. dem Pfad und dem Namen der Image-Datei ein.

INFO: Mit der Schaltfläche **Voreinstellung** können Sie die eingegebenen Werte wieder auf die Standardwerte zurücksetzen.

---

b) Geben Sie im Feld **Benutzername** den Benutzernamen und im Feld **Passwort** das Passwort für den Zugriff auf den lokalen Webserver ein.

c) Aktivieren Sie das Kontrollkästchen **Software Update Information** und geben Sie unter Startzeit einen **Zeitpunkt** an, zu der auf dem oben angegebenen Server nach einer neueren Software gesucht werden soll.

d) Wenn Sie für die Übertragung einen Proxy-Server verwenden, aktivieren Sie das Kontrollkästchen **Proxy verwenden** und geben Sie die Daten für den Proxy-Server ein.

6) Klicken Sie auf **Übernehmen**. Die eingegebenen Zugangsdaten des lokalen Webservers werden als Standard übernommen.

Liegt auf dem lokalen Webserver bereits eine neue Image-Datei, wird die Software-Aktualisierung eingeleitet und es erscheint die Lizenzvereinbarung (siehe *Wie Sie das System über einen Webserver aktualisieren*). Der Start der Software-Aktualisierung kann aber bei Bedarf noch verhindert werden.

24.3.2 Update des Kommunikationssystems

Mit dem Update des Kommunikationssystems wird die Software des Kommunikationssystems aktualisiert und zusätzlich die auf dem Kommunikationssystem gespeicherten Software-Images der Systemtelefone. Damit ist ein komplettes Update aller Systemkomponenten schnell und einfach durchzuführen.

Vor jeder Software-Aktualisierung sollten die Konfigurationsdaten des Kommunikationssystems gesichert werden (*Sichern und Wiederherstellen*).

Aktualisierung über Webserver

Bei der Software-Aktualisierung über einen Webserver wird standardmäßig auf den Software-Server (Internet-Webserver) zugegriffen.

Wird ein lokaler Webserver verwendet, muss die Image-Datei auf dem lokalen Webserver abgelegt sein.

Für ein Kommunikationssystem ohne UC Booster Card ist es egal, ob eine Image-Datei für ein System ohne oder mit UC Booster Card verwendet wird. Es werden nur die benötigten Komponenten installiert.

Nachdem automatisch eine Verbindung zum Webserver aufgebaut wurde, wird geprüft, ob neue Software-Updates vorliegen. Einzelne Pakete des Software-Updates können bei Systemen ohne UC Booster abgewählt werden, um die Downloadzeit zu verringern. Es werden auch nur die Pakete übertragen, die sich gegenüber der installierten Software-Version geändert haben. Startzeitpunkt der Software-Übertragung und Startzeitpunkt der Software-Aktivierung können ausgewählt werden. Wird der Zeitpunkt der Software-Aktivierung erreicht, obwohl das Software-Update noch nicht komplett auf das System übertragen ist, wird die Aktivierung nicht automatisch durchgeführt. Es muss manuell ein neuer Aktivierungszeitpunkt festgelegt werden.

Aktualisierung über USB-Medium

Die Image-Datei ist auf einem USB-Medium gespeichert. Das USB-Medium wird in die USB-Server-Schnittstelle des Kommunikationssystems gesteckt. Diese Art der Aktualisierung kann nur von einem Administrator mit dem Profil **Expert** durchgeführt werden und ist nicht möglich für OpenScape Business S und OpenScape Business UC Booster Server.

Aktualisierung über Datei-Upload

Die Image-Datei befindet sich in einem Verzeichnis im internen Netz oder auf dem Admin-PC.

Aktualisierung über USB-Medium ohne WBM-Zugriff

Das Kommunikationssystem kann direkt ohne WBM-Zugang über ein USB-Medium aktualisiert werden. Dazu muss das USB-Medium in der USB-Server-Schnittstelle des Systems gesteckt werden und die Image-Datei auf der obersten Verzeichnisebene des USB-Mediums liegen. Wird bei gestecktem USB-Medium ein Reset des Kommunikationssystems durchgeführt, wird automatisch das Software-Update gestartet. Diese Art der Aktualisierung ist nicht möglich bei OpenScape Business S. Bei einem System mit OpenScape Business UC Booster Server muss der Server zusätzlich aktualisiert werden.

Aktualisierung des UC Booster Servers

Wird zusätzlich zum Kommunikationssystem ein UC Booster Server betrieben, so muss bei einem Update der System-Software auch die Kommunikationssoftware des UC Booster Servers aktualisiert werden. Die Software des Kommunikationssystems und des UC Booster Servers sollten immer auf dem gleichen Stand sein. Der Software-Update des UC Booster Servers erfolgt identisch zum Software-Update des Kommunikationssystems, nur dass der Administrator beim Aufruf des WBM nicht die IP-Adresse des Kommunikationssystems angibt, sondern die IP-Adresse des Linux-Servers.

24.3.2.1 Wie Sie das System über einen Webserver aktualisieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.
- Auf der Startseite des WBM wird angezeigt, dass eine neue Softwareversion vorliegt.
- Ein Zugang zum Webserver ist vorhanden. Standardmäßig wird die Verbindung zum Internet-Webserver aufgebaut. Stattdessen kann ein lokaler Webserver konfiguriert werden (siehe *Nutzung eines lokalen Webservers*).
- Wird das Update über einen lokalen Webserver ausgeführt, muss die aktuellste Image-Datei auf dem lokalen Webserver abgelegt sein.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Startseite** und zuerst auf den Link **Zum Inhalt können Sie sich hier informieren: Link**. Es öffnet sich eine PDF-Datei mit wichtigen Hinweisen zu der neuen Softwareversion. Lesen Sie sich die Informationen durch und berücksichtigen Sie die Informationen zur Hochrüstung des Systems. Schließen Sie das Fenster anschließend.

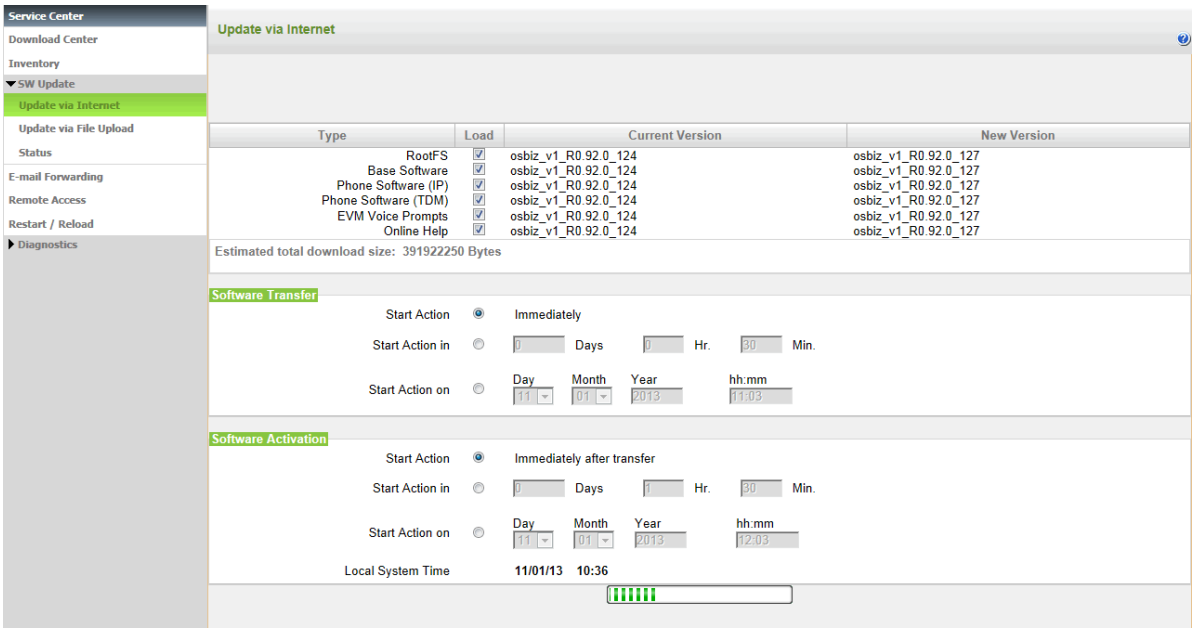
2) Klicken Sie in der Navigationsleiste auf **Service-Center**.

3) Klicken Sie im Navigationsbaum auf **Software Update > Update via Internet**. Es wird Ihnen die aktuell installierte Softwareversion angezeigt.

4) Klicken Sie auf **OK & Weiter**.

5) Lesen Sie sich die Lizenzvereinbarung (EULA) durch und aktivieren Sie anschließend das Optionsfeld **Ich stimme der Lizenzvereinbarung zu**.

6) Klicken Sie auf **OK & Weiter**.



7) Deaktivieren Sie bei Bedarf in der Spalte **Laden** die Pakete, die nicht aktualisiert werden sollen. Das ist z. B. sinnvoll bei langsamen Internet-Verbindungen oder Software-Aktualisierungen über ISDN.

8) Wählen Sie die Zeitpunkte für Software-Übertragung und Software-Aktivierung aus:

- **Start der Aktion - Sofort / Sofort nach der Übertragung**: die Software wird sofort übertragen bzw. sofort nach der Übertragung aktiviert. Das Software-Update wird im Hintergrund in das Kommunikationssystem geladen. Nach zwei Neustarts ist die Software aktualisiert.
- **Start der Aktion in**: die Software wird nach Ablauf einer bestimmten Zeit übertragen bzw. aktiviert. Geben Sie dazu den Zeitraum in Tagen, Stunden und Minuten an.
- **Start der Aktion am**: die Software wird zu einem bestimmten Zeitpunkt übertragen bzw. aktiviert. Geben Sie dazu Datum und Uhrzeit des Zeitpunkts an.

INFO: Wird der Zeitpunkt der Software-Aktivierung erreicht, obwohl das Software-Update noch nicht komplett auf das System übertragen ist, wird die Aktivierung nicht automatisch durchgeführt. Es muss manuell ein neuer Aktivierungszeitpunkt festgelegt werden.

---

9) Klicken Sie auf **OK & Weiter**. Das Software-Update wird zu den von Ihnen konfigurierten Zeitpunkten im Hintergrund in das System geladen und

aktiviert. Für die Software-Aktivierung werden automatisch hintereinander zwei Neustarts durchgeführt.

INFO: Sie können das Browser-Fenster jederzeit schließen.

10) Den aktuellen Status des Updates können Sie mit dem WBM unter **Service-Center > Software-Update > Status** abfragen.

24.3.2.2 Wie Sie das System über ein USB-Medium aktualisieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.
- Das USB-Medium muss mit FAT32 formatiert sein.
- Eine aktuelle Image-Datei ist als tar-Datei auf dem USB-Medium gespeichert. Es können auch mehrere Image-Dateien in unterschiedlichen Verzeichnissen abgelegt sein.
- Hat das USB-Medium mehrere Partitionen, muss die Image-Datei in der ersten Partition abgelegt sein.

Schritt für Schritt

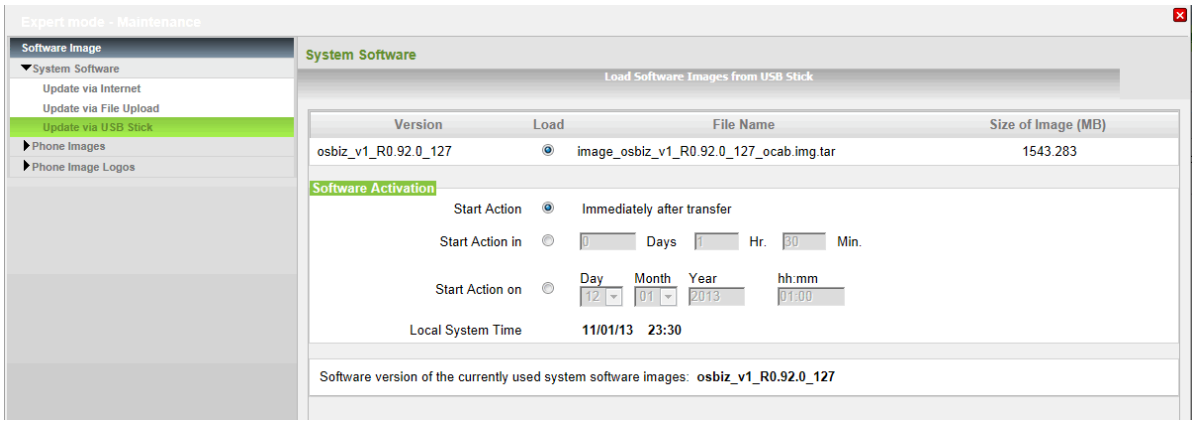
1) Stecken Sie das USB-Medium in die USB-Server-Schnittstelle des Mainboards.

2) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

3) Klicken Sie im Navigationsbaum auf **Wartung > Software-Image**.

4) Klicken Sie im Menübaum auf **System-Software**.

5) Klicken Sie auf **Update via USB-Stick**. Es werden Ihnen alle auf dem USB-Medium gespeicherten, gültigen Image-Dateien mit Versionsnummer und Dateiname angezeigt.



6) Wenn mehrere Image-Dateien gespeichert sind, wählen Sie die gewünschte Image-Datei aus, ansonsten ist die Image-Datei automatisch markiert.

7) Wählen Sie den Zeitpunkt für die Software-Aktivierung aus:

- **Start der Aktion - Sofort nach der Übertragung**: die Software wird sofort nach der Übertragung in das Kommunikationssystem aktiviert.
- **Start der Aktion in**: die Software wird sofort in das Kommunikationssystem übertragen. Nach Ablauf einer bestimmten Zeit wird die Software aktiviert. Geben Sie dazu den Zeitraum in Tagen, Stunden und Minuten an.
- **Start der Aktion am**: die Software wird sofort in das Kommunikationssystem übertragen. Zu einem bestimmten Zeitpunkt wird die Software aktiviert. Geben Sie dazu Datum und Uhrzeit des Zeitpunkts an.

8) Klicken Sie auf **Laden**. Die Image-Datei wird in das Kommunikationssystem übertragen und auf Konsistenz überprüft. Für beide Vorgänge werden mehrere Minuten benötigt. Während dieser Zeit muss das USB-Medium gesteckt bleiben.

9) Ziehen Sie das USB-Medium, sobald das WBM Sie darauf hinweist, und klicken Sie auf **Beenden**. Zum angegebenen Zeitpunkt der Software-Aktivierung werden automatisch hintereinander zwei Neustarts durchgeführt.

10) Den aktuellen Status des Updates können Sie mit dem WBM unter **Service-Center > Software-Update > Status** abfragen.

24.3.2.3 Wie Sie das System über einen Datei-Upload aktualisieren

Voraussetzungen

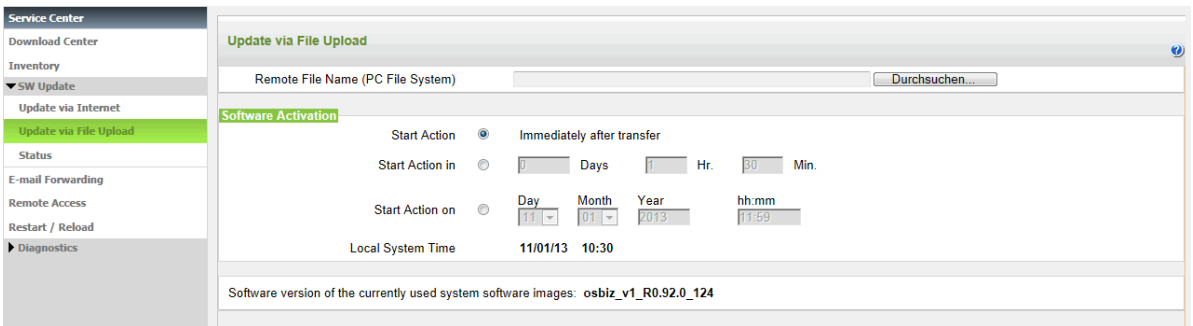
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.
- Die Image-Datei ist als tar-Datei im internen Netz oder direkt auf dem Admin-PC gespeichert und der Ablageort ist bekannt. Ist eine tgz-Datei gespeichert, muss die tar-Datei aus der tgz-Datei entpackt werden.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Software Update > Update via File Upload**. Es wird Ihnen die aktuell installierte Softwareversion angezeigt.

3) Klicken Sie auf **OK & Weiter**.



4) Navigieren Sie mit der Schaltfläche **Durchsuchen** zum Ablageort der Image-Datei (`*.tar`).

5) Wählen Sie den Zeitpunkt für die Software-Aktivierung aus:

- **Start der Aktion - Sofort nach der Übertragung**: die Software wird sofort im Hintergrund in das Kommunikationssystem übertragen. Nach zwei Neustarts ist die Software aktualisiert.
- **Start der Aktion in**: die Software wird sofort im Hintergrund in das Kommunikationssystem übertragen. Nach Ablauf einer bestimmten Zeit wird die Software aktiviert. Geben Sie dazu den Zeitraum in Tagen, Stunden und Minuten an.
- **Start der Aktion am**: die Software wird sofort im Hintergrund in das Kommunikationssystem übertragen. Zu einem bestimmten Zeitpunkt wird die Software aktiviert. Geben Sie dazu Datum und Uhrzeit des Zeitpunkts an.

6) Klicken Sie auf **OK & Weiter**. Die Image-Datei wird in das Kommunikationssystem übertragen und auf Konsistenz überprüft. Für beide Vorgänge werden mehrere Minuten benötigt.

> ***INFO:*** Wenn Sie das Browser-Fenster während des Software-Transfers schließen, wird der Vorgang abgebrochen. Während des Konsistenz-Checks können Sie mit dem WBM weiterarbeiten oder es schließen.

7) Soll die Software sofort aktiviert werden, werden nach erfolgreicher Konsistenz-Prüfung automatisch hintereinander zwei Neustarts durchgeführt.

8) Soll die Software nicht sofort aktiviert werden, klicken Sie nach erfolgreicher Übertragung auf **Beenden**. Zum Zeitpunkt der Software-Aktivierung werden automatisch hintereinander zwei Neustarts durchgeführt.

9) Den aktuellen Status des Updates können Sie mit dem WBM unter **Service-Center > Software-Update > Status** abfragen.

24.3.2.4 Wie Sie das System über ein USB-Medium ohne WBM-Zugriff aktualisieren

Voraussetzungen

- Das USB-Medium muss mit FAT32 formatiert sein.
- Eine aktuelle Image-Datei ist als tar-Datei in der obersten Verzeichnisebene des USB-Mediums gespeichert. Dort darf nur eine Image-Datei abgelegt sein.
- Hat das USB-Medium mehrere Partitionen, muss die Image-Datei in der ersten Partition abgelegt sein.
- Die Software-Version der Image-Datei muss neuer sein als die Software-Version des Systems. Vorsicht: es wird auch auf ältere Software-Versionen aktualisiert.
- Das Kommunikationssystem ist gestartet.

Schritt für Schritt

1) Stecken Sie das USB-Medium in die USB-Server-Schnittstelle des Mainboards.

2) Drücken Sie den Reset-Knopf zwischen 1 bis 4 Sekunden lang. Das System fährt herunter und beginnt einen Neustart.

Während des Hochlaufs wird die Software geprüft. Enthält das USB-Medium eine geeignete Image-Datei, wird die Datei auf das Kommunikationssystem geladen. Die rote LED blinkt dabei im 1Hz-Takt (0,5s an / 0,5s aus). Ist der Kopiervorgang beendet, wird die Software entpackt und die Kundendaten automatisch übernommen. Dabei blinkt die rote LED im 5Hz-Takt (100ms an / 100ms aus).

3) Entfernen Sie das USB-Medium, wenn die rote LED im 5Hz-Takt blinkt.

4) Abschließend führt das System hintereinander automatisch zwei Neustarts durch. Wenn die grüne LED im 1Hz-Takt blinkt (0,5s an / 0,5s aus), ist das System wieder betriebsbereit.

24.3.3 Update der Systemtelefone

Die Software der Systemtelefone wird über eine Image-Datei aktualisiert. Für jeden Systemtelefontyp gibt es eine eigene Image-Datei, die die Telefon-Software dieses Typs enthält. Diese Image-Dateien sind in der Software des Kommunikationssystems enthalten und werden beim Update automatisch auf das Kommunikationssystem geladen.

Die IP-Systemtelefone werden standardmäßig automatisch mit der aktuellen Software versorgt. Eine vom Standard abweichende Telefon-Software kann der Administrator über das WBM manuell auf alle einem Typ zugehörigen IP-Systemtelefone übertragen. Das Update der Software für die UP0-Systemtelefone wird mit dem Manager E durchgeführt.

Ist eine Telefon-Software (Image-Datei) im WBM als Standard markiert, wird dieses Image automatisch auf jedes diesem Typ zugehörige IP-Systemtelefon übertragen, wenn es sich zum ersten Mal am System anmeldet.

Achten Sie bei einer manuellen Aktualisierung darauf, dass die Software der Systemtelefone zur Software-Version des Kommunikationssystems kompatibel ist (siehe Release Note).

24.3.3.1 Wie Sie die Telefonsoftware ins System laden

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.
- Die Image-Dateien sind im lokalen Netz gespeichert und der Ablageort ist bekannt. Für jeden Systemtelefontyp wird eine eigene Image-Datei benötigt.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung > Software-Image**.
3) Klicken Sie im Menübaum auf **Telefon-Images**.
4) Klicken Sie auf **Laden**. Es wird Ihnen eine Liste der aktuell im Kommunikationssystem vorhandenen Image-Dateien angezeigt.
5) Navigieren Sie unter **Remote-Dateiname (PC-Dateisystem)** mit **Durchsuchen** zum Ablageort der Image-Datei (`*.app`).
6) Klicken Sie auf **Laden**. Die Image-Datei wird geladen und auf Fehler geprüft.

   INFO: Bei einem Fehler erhalten Sie eine Fehlermeldung. Prüfen Sie Ihre Eingaben und wiederholen Sie die Schritte 5 bis 6.

7) Bestätigen Sie bei erfolgreicher Prüfung mit **OK**. Die Image-Datei wird in die Liste der aktuell im Kommunikationssystem vorhandenen Image-Dateien aufgenommen.
8) Wenn Sie weitere Image-Dateien für andere Systemtelefontypen laden wollen, wiederholen Sie die Schritte 5 bis 7.

24.3.3.2 Wie Sie die Telefonsoftware an Systemtelefone verteilen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung > Software-Image**.
3) Klicken Sie im Menübaum auf **Telefon-Images**.
4) Wenn Sie ein Telefon-Image an alle Systemtelefone eines Typs verteilen wollen:
   a) Klicken Sie auf **Verteilen**. Es wird Ihnen eine Liste der aktuell im Kommunikationssystem vorhandenen Image-Dateien angezeigt.
   b) Aktivieren Sie das Kontrollkästchen **Verteilen** bei dem oder den gewünschten Telefon-Images.
5) Wenn Sie ein Telefon-Image an ein bestimmtes Systemtelefon verteilen wollen:
   a) Klicken Sie auf **Verteilen pro Endgerät**. Es wird Ihnen eine Liste der Systemtelefone angezeigt.
   b) Wählen Sie aus der Aufklappliste **verteilbare Software** für das oder die gewünschten Systemtelefone das Telefon-Image aus.

6) Klicken Sie auf **Übernehmen**.

24.3.3.3 Wie Sie die Telefonsoftware löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung > Software-Image**.

3) Klicken Sie im Menübaum auf **Telefon-Images**.

4) Klicken Sie auf **Laden**. Es wird Ihnen eine Liste der aktuell im Kommunikationssystem vorhandenen Image-Dateien angezeigt.

5) Aktivieren Sie in der Zeile des zu löschenden Telefon-Images das Kontrollkästchen **Löschen**.

6) Wenn Sie weitere Telefon-Images löschen wollen, wiederholen Sie den vorherigen Schritt.

7) Klicken Sie auf **Löschen**. Alle markierten Telefon-Images werden aus dem Kommunikationssystem gelöscht.

24.3.3.4 Wie Sie die automatische Verteilung der Telefonsoftware aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung > Software-Image**.

3) Klicken Sie im Menübaum auf **Telefon-Images**.

4) Klicken Sie auf **Verteilen**. Es wird Ihnen eine Liste der aktuell im Kommunikationssystem vorhandenen Image-Dateien angezeigt.

5) Wenn die Telefonsoftware automatisch an die Systemtelefone übertragen werden soll, aktivieren Sie in der Zeile der gewünschten Image-Datei das Kontrollkästchen **Standard** (Standardeinstellung).

6) Wenn die Telefonsoftware nicht automatisch an die Systemtelefone übertragen werden soll, deaktivieren Sie in der Zeile der gewünschten Image-Datei das Kontrollkästchen **Standard**.

7) Klicken Sie auf **Übernehmen**.

24.3.3.5 Wie Sie ein optiPoint WL2 professional von HFA auf SIP umrüsten

Voraussetzungen

- Die Telefon-Software liegt als Image-Datei in der Zwischenversion `prep70_39.img` vor.
- Die Telefon-Software liegt als Image-Datei in der endgültigen Version vor, z. B. Standard-Image-Datei `swup_70-000-52.img`.
- Die Benutzerdaten des WL2 und die WLAN-Zugangsdaten liegen Ihnen vor.
- Ein neuer SIP-Teilnehmer wurde im WBM des Systems inkl. der SIP-Zugangsdaten eingerichtet und lizenziert. Die im System vergebenen SIP-Zugangsdaten liegen Ihnen vor.

Schritt für Schritt

1) Upgrade auf die Zwischenversion:

a) Installieren Sie zuerst die Zwischenversion `prep70_39.img` mittels WBM des WL2 oder DLS. Der Upgrade-Fortschritt wird auf dem Telefondisplay angezeigt.

b) Folgen sie den Anweisungen im Display und warten sie, bis das WL2 neu gestartet ist.

c) Bestätigen Sie nach erfolgreichem Start die Meldung **Temp. SW only - Please Update!** mit **OK**.

2) Upgrade auf die endgültige Version:

a) Installieren Sie nun eine Standard-Image-Datei, z. B. `swup_70-000-052.img`. Aus Sicherheitsgründen werden während des Upgrades keine Einstellungen und Benutzerdaten geändert. Der Upgrade-Fortschritt wird auf dem Telefondisplay angezeigt.

b) Folgen sie den Anweisungen im Display und warten sie, bis das WL2 neu gestartet ist.

3) Aktivieren Sie nach erfolgreichem Start die Standard-Telefoneinstellungen manuell über das WBM des WL2:

- 1. Möglichkeit: Navigieren Sie im WBM zu **System Settings > Reset User Data > User Settings Clear**.
- 2. Möglichkeit: Navigieren Sie im WBM zu **Factory Reset > Restore the factory defaults**.

HINWEIS: Ihre Benutzerdaten und die WLAN-Zugangsdaten gehen verloren!

---

4) Geben Sie die WLAN-Zugangsdaten am Telefon ein, um das Telefon ins Kunden-LAN einzubinden.

5) Geben Sie die SIP-Zugangsdaten am Telefon ein, damit sich das Telefon als SIP-Teilnehmer am System anmelden kann.

6) Setzen Sie im WBM des WL2 das Optionsfeld **Network > SIP advanced > Auto Answer** auf **On**, um die Funktionalität des Telefons im Zusammenspiel mit den UC Suite Clients sicherzustellen.

24.3.4 Software-Status

Der Software-Status gibt Auskunft über den Softwarestand und die Aktualisierung der Software.

Folgende Stati können angezeigt werden:

- aktuelle Version der Software
- aktuellere Version liegt zur Aktualisierung vor
- Zeitpunkt, zum die Software-Aktualisierung durchgeführt wird
- neue Software wird gerade in das System geladen
- Ladevorgang war erfolgreich oder fehlerhaft

24.3.4.1 Wie Sie den Software-Status abfragen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

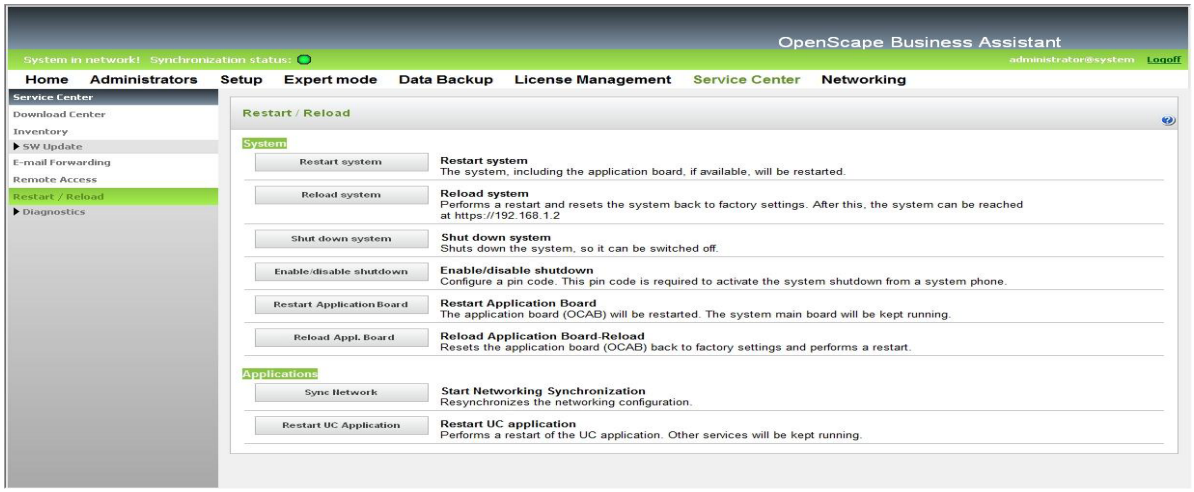
2) Klicken Sie im Navigationsbaum auf **Software Update > Status**. Es wird Ihnen die aktuelle Version der Software angezeigt. Diese Information wird Ihnen auch auf der Startseite des WBM angezeigt.

Falls im Hintergrund gerade ein Software-Update läuft, wird Ihnen das hier mitgeteilt.

Falls ein neues Software-Update auf dem Webserver vorliegt, wird Ihnen das hier mitgeteilt. Diese Information wird Ihnen auch auf der Startseite des WBM angezeigt.

24.4 Restart, Reload, Shutdown

Über die zugehörigen Funktionen kann ein Restart (Neustart) und ein Reload des OpenScape Business Kommunikationssystems oder der UC Booster Card ausgelöst werden sowie OpenScape Business X kontrolliert herunterfahren werden (Shutdown). Darüber hinaus kann ein Restart (Neustart) der UC Applikation (UC Smart oder UC Suite) ausgelöst werden. Um das kontrollierte Herunterfahren von OpenScape Business X über ein Systemtelefon zu ermöglichen, kann eine PIN definiert werden.



Restart und Reload des UC Booster Servers

Wird zusätzlich zum Kommunikationssystem ein UC Booster Server betrieben, so kann auch die Kommunikationssoftware des UC Booster Servers neu gestartet oder reloadet werden. Der Restart/Reload des UC Booster Servers erfolgt identisch zum Restart/Reload des Kommunikationssystems, nur dass der Administrator beim Aufruf des WBM nicht die IP-Adresse des Kommunikationssystems angibt, sondern die IP-Adresse des Linux-Servers.

24.4.1 Restart (Neustart) von OpenScape Business

Über die Funktion **System neu starten** kann ein kontrollierter Restart (Neustart) von OpenScape Business ausgelöst werden.

Folgende Unterschiede sind zu beachten:

- OpenScape Business S und OpenScape Business X
  Es erfolgt ein kontrollierter Restart (Neustart) des Kommunikationssystems. Nach dem Hochlauf ist das Kommunikationssystem wieder betriebsbereit.
  Die Hochlaufzeit ist abhängig vom Systemausbau und dem OpenScape Business-Vernetzungsszenario.
  Ist OpenScape Business X3/X5/X8 mit einer UC Booster Card (Application Board OCAB) bestückt, erfolgt auch ein kontrollierter Restart (Neustart) der UC Applikation (UC Smart oder UC Suite).
- OpenScape Business UC Booster Server (Application Server)
  Es erfolgt ein kontrollierter Restart (Neustart) des OpenScape Business-Anteils und der UC Applikation (UC Suite). Nach dem Hochlauf ist die UC Applikation wieder betriebsbereit.

Bei einem Restart werden die Verbindungen zu allen aktiven Anwendungen, wie zum Beispiel myPortal for Desktop und myAttendant, getrennt. Nach dem Hochlauf werden alle Verbindungen automatisch wiederhergestellt.

24.4.1.1 Wie Sie einen Restart (Neustart) von OpenScape Business auslösen

Mit der Funktion **System neu starten** können Sie einen Restart (Neustart) von OpenScape Business auslösen.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

> ***INFO:*** Bei einem Restart werden die Verbindungen zu allen aktiven Anwendungen, wie zum Beispiel myPortal for Desktop und myAttendant, getrennt. Nach dem Hochlauf werden alle Verbindungen automatisch wiederhergestellt.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Restart / Reload**.

3) Klicken Sie auf **System neu starten** und anschließend auf **OK**. OpenScape Business führt einen Restart (Neustart) durch.

OpenScape Business S und OpenScape Business X: Nach dem Hochlauf ist das Kommunikationssystem wieder betriebsbereit.

OpenScape Business UC Booster Server: Nach dem Hochlauf ist die UC Applikation (UC Suite) wieder betriebsbereit.

24.4.2 Reload von OpenScape Business

Über die Funktion **System-Reload ausführen** kann ein Reload von OpenScape Business ausgelöst werden.

Folgende Unterschiede sind zu beachten:

- OpenScape Business S und OpenScape Business X
  Es erfolgt ein Reload des Kommunikationssystems. Nach dem anschließenden Hochlauf befindet sich das Kommunikationssystem im Grundzustand:
  - Alle länder- und kundenspezifischen Einstellungen wurden gelöscht (System-Länderkennzeichen = Deutschland).
  - Das Kommunikationssystem hat die Standard-IP-Adresse 192.168.1.2 und den internen IP-Adressbereich 192.168.3.xxx.
  - Die Lizenzierung bleibt erhalten.

  Die Hochlaufzeit ist abhängig vom Systemausbau.
- OpenScape Business UC Booster Server
  Es erfolgt ein Reload des OpenScape Business-Anteils. Nach dem anschließenden Hochlauf befindet sich der OpenScape Business-Anteil im Grundzustand:

– Alle kundenspezifischen Einstellungen des OpenScape Business-Anteils (zum Beispiel das Benutzerverzeichnis) wurden gelöscht.
– Die Lizenzierung bleibt erhalten.

Das Betriebssystem wird nicht zurückgesetzt.

24.4.2.1 Wie Sie einen Reload von OpenScape Business auslösen

Mit der Funktion **System-Reload ausführen** können Sie einen Reload von OpenScape Business auslösen.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.
- OpenScape Business S und OpenScape Business X: Die Konfigurationsdaten des Kommunikationssystems wurden in einem Backup-Set gesichert.

  HINWEIS: Durch einen Reload wird das Kommunikationssystem in den Grundzustand versetzt. Alle länder- und kundenspezifischen Einstellungen werden gelöscht (System-Länderkennzeichen = Deutschland). Das Kommunikationssystem erhält die Standard-IP-Adresse 192.168.1.2.

- OpenScape Business UC Booster Server: Die Konfigurationsdaten des OpenScape Business-Anteils wurden in einem Backup-Set gesichert.

  HINWEIS: Durch einen Reload wird der OpenScape Business-Anteil in den Grundzustand versetzt. Alle kundenspezifischen Einstellungen des OpenScape Business-Anteils (zum Beispiel das Benutzerverzeichnis) werden gelöscht.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Restart / Reload**.

3) Klicken Sie auf **System-Reload ausführen** und anschließend auf **OK**. OpenScape Business führt einen Reload durch.

INFO: OpenScape Business S und OpenScape Business X: Nach dem anschließenden Hochlauf befindet sich das Kommunikationssystem im Grundzustand. Nach Konfiguration der Grundeinstellungen über den Wizard Erstinstallation können die gesicherten länder- und kundenspezifischen Daten wieder geladen werden. Informationen zur Vorgehensweise siehe *Wiederherstellen*.

OpenScape Business UC Booster Server: Nach dem anschließenden Hochlauf befindet sich der OpenScape Business-Anteil

im Grundzustand. Die gesicherten kundenspezifischen Daten können wieder geladen werden. Informationen zur Vorgehensweise siehe *Wiederherstellen*.

24.4.3 Shutdown (Herunterfahren) von OpenScape Business X

Über die Funktion **System herunterfahren** kann ein kontrolliertes Herunterfahren der Kommunikationssysteme OpenScape Business X veranlasst werden.

24.4.3.1 Wie Sie OpenScape Business X herunterfahren

Mit der Funktion **System herunterfahren** können Sie ein kontrolliertes Herunterfahren der Kommunikationssysteme OpenScape Business X veranlassen.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Restart / Reload**.

3) Klicken Sie auf **System herunterfahren** und anschließend auf **OK**. Das Kommunikationssystem wird kontrolliert heruntergefahren.

INFO: OpenScape Business X1/X3/X5: Das anschließende Hochfahren des Kommunikationssystems ist ausschließlich durch Ziehen und anschließendes Stecken des Netzsteckers möglich.

OpenScape Business X8: Das anschließende Hochfahren des Kommunikationssystems ist ausschließlich durch Ausschalten und anschließendes Wiedereinschalten aller Stromversorgungen LUNA2 möglich.

24.4.4 PIN für das kontrollierte Herunterfahren (Shutdown) von OpenScape Business X

Die Aktivierung des Shutdowns über ein Systemtelefon ist PIN-geschützt.

Bei der Aktivierung über ein Systemtelefon muss immer die im Kommunikationssystem konfigurierte PIN eingegeben werden. Die Konfiguration dieser PIN erfolgt durch einen Administrator mit dem Profil **Advanced**.

24.4.4.1 Wie Sie eine PIN für das kontrollierte Herunterfahren (Shutdown) von OpenScape Business X konfigurieren

Die PIN gilt für die Aktivierung eines Shutdowns über ein Systemtelefon.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Restart / Reload**.

3) Klicken Sie auf **Shutdown aktivieren/deaktivieren**.

4) Geben Sie im Feld **PIN** die gewünschte sechsstellige PIN ein.

5) Klicken Sie auf **Sichern** und anschließend auf **OK**.

Nächste Schritte

Die Aktivierung eines Shutdowns über ein Systemtelefon erfolgt durch Eingabe der entsprechenden Kennzahl (Standardkennzahl = *997) und anschließender Eingabe der sechsstelligen PIN.

24.4.5 Restart (Neustart) der UC Booster Card (Application Board OCAB)

Über die Funktion **Application Board neu starten** können Sie als Administrator einen kontrollierten Restart (Neustart) des Application Boards OCAB inklusive der UC Applikation (UC Smart oder UC Suite) auslösen.

Bei einem Restart werden die Verbindungen zu allen aktiven Anwendungen, wie zum Beispiel myPortal for Desktop und myAttendant, getrennt. Nach dem Hochlauf werden alle Verbindungen automatisch wiederhergestellt.

Darüber hinaus wird der integrierte XMPP-Server, die CSTA-Schnittstelle, der Presence Manager, der Announcement Player, die Media Extension Bridge, der Open Directory Service und der Gate View Server neu gestartet.

24.4.5.1 Wie Sie einen Restart (Neustart) der UC Booster Card (Application Board OCAB) auslösen

Mit der Funktion **Application Board neu starten** können Sie einen kontrollierten Restart (Neustart) des Application Boards OCAB inklusive der UC Applikation (UC Smart oder UC Suite) auslösen.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

> ***INFO:*** Bei einem Restart werden die Verbindungen zu allen aktiven Anwendungen, wie zum Beispiel myPortal for Desktop und myAttendant, getrennt. Nach dem Hochlauf werden alle Verbindungen automatisch wiederhergestellt.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Restart / Reload**.

3) Klicken Sie auf **Application Board neu starten** und anschließend auf **OK**. Die UC Booster Card (Application Board OCAB) führt einen Restart (Neustart) durch.

24.4.6 Reload der UC Booster Card (Application Board OCAB)

Über die Funktion **UC Booster Card Reload ausführen** kann ein Reload des Application Boards OCAB inklusive der UC Applikation (UC Smart oder UC Suite) ausgelöst werden.

Der Reload der UC Booster Card dient dazu, die Karte auf die Werkseinstellungen zurückzusetzen und sie anschließend aus dem System zu entfernen. Dies kann z. B. notwendig werden, wenn die Karte nicht mehr in diesem System verwendet werden soll, weil auf den UC Booster Server umgestiegen oder die Karte in einem anderen/neuen OpenScape Business System eingesetzt werden soll.

Alle kundenspezifischen Daten und alle Diagnose-Daten werden auf der UC Booster Card gelöscht und das System wird heruntergefahren. Anschließend wird das System vom Stromnetz genommen und die UC Booster Card entfernt.

Nachdem die UC Booster Card entfernt und das System neu hochgefahren wurde, ist ein neues Backup-Set zu erstellen, da sich die Konfigurationsdaten geändert haben und das alte Backup-Set nicht mehr kompatibel ist. Wurde vorher die Festplatte der UC Booster Card als Backup-Medium verwendet, muss nun ein anderes Backup-Medium ausgewählt werden, wie z. B. ein Netzlaufwerk, ein USB-Medium oder ein FTP-/FTPS-Server (siehe auch *Sichern und Wiederherstellen*).

24.4.6.1 Wie Sie einen Reload der UC Booster Card (Application Board OCAB) auslösen

Mit der Funktion **UC Booster Card Reload ausführen** können Sie einen Reload des Application Boards OCAB inklusive der UC Applikation (UC Smart oder UC Suite) auslösen.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Restart / Reload**.

3) Klicken Sie auf **UC Booster Card Reload ausführen** und anschließend auf **OK**. Sie werden vom WBM abgemeldet. Die Karte wird auf die Werkseinstellungen zurückgesetzt und das System anschließend heruntergefahren.

4) Sobald die grüne RUN LED des Mainboards und die Controller-LEDs der UC Booster Card komplett erloschen sind, nehmen Sie das System vom Stromnetz und entfernen Sie die UC Booster Card (siehe *Servicedokumentation, Montage der Hardware*).

5) Erstellen Sie ein neues Backup-Set, nachdem das System neu hochgefahren ist, da sich die Konfigurationsdaten geändert haben und das alte Backup-Set nicht mehr kompatibel ist (siehe auch *Sichern und Wiederherstellen*).

24.4.7 Restart (Neustart) der UC Applikation

Über die Funktion **UC Application neu starten** können Sie als Administrator einen kontrollierten Restart (Neustart) der UC Applikation (UC Smart oder UC Suite) auslösen.

Bei einem Restart der UC Applikation werden die Verbindungen zu allen aktiven Anwendungen, wie zum Beispiel myPortal for Desktop, myPortal Smart und myAttendant, getrennt. Nach dem Hochlauf werden alle Verbindungen automatisch wiederhergestellt.

24.4.7.1 Wie Sie einen Restart (Neustart) der UC Applikation auslösen

Mit der Funktion **UC Application neu starten** können Sie einen Restart (Neustart) der UC Applikation (UC Smart oder UC Suite) auslösen.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

INFO: Bei einem Restart werden die Verbindungen zu allen aktiven Anwendungen, wie zum Beispiel myPortal for Desktop, myPortal Smart und myAttendant, getrennt. Nach dem Hochlauf werden alle Verbindungen automatisch wiederhergestellt.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Restart / Reload**.
3) Klicken Sie auf **UC Application neu starten** und anschließend auf **OK**. Die UC Applikation führt einen Restart (Neustart) durch.

24.4.8 Restart (Neustart) der Web Services

Über die Funktion **Restart Web Services** können Sie als Administrator einen kontrollierten Restart (Neustart) der Web Services der Kommunikationssysteme OpenScape Business S und OpenScape Business X3/X5/X8 (mit UC Booster Card (Application Board OCAB)) und des OpenScape Business UC Booster Servers auslösen.

Bei einem Restart der Web Services werden die Web Services neu gestartet. Bestehende Sessions der Clients myPortal for Mobile, myPortal to go und myPortal for OpenStage werden beendet.

Darüber hinaus wird der integrierte XMPP-Server und der Open Directory Service neu gestartet.

24.4.8.1 Wie Sie einen Restart (Neustart) der Web Services auslösen

Mit der Funktion **Restart Web Services** können Sie einen Restart (Neustart) der Web Services der Kommunikationssysteme OpenScape Business S und OpenScape Business X3/X5/X8 (mit UC Booster Card (Application Board OCAB)) und des OpenScape Business UC Booster Servers auslösen.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Restart / Reload**.
3) Klicken Sie auf **Restart Web Services** und anschließend auf **OK**. Die Web Services führen einen Restart (Neustart) durch.

24.5 Inventory-Management

Unter Inventory-Management versteht man die Ermittlung des aktuellen Status der Kommunikationssysteme OpenScape Business Xund OpenScape Business S und der Hardware-Konfiguration der Kommunikationssysteme OpenScape Business X.

24.5.1 Systemstatus

Den aktuellen Status der Kommunikationssysteme OpenScape Business X und OpenScape Business S kann ein Administrator mittels WBM ermitteln. Abgerufen werden können Informationen über den Status der Teilnehmer, des Verbindungsaufbaus, der ITSPs und der VPNs und die Liste der konfigurierten IP-Adressen.

Teilnehmer-Status

Der Teilnehmer-Status ermöglicht die Abfrage folgender Informationen über die eingerichteten Teilnehmer:

- Rufnummer
- Name
- Endgeräte Typ
- IP-Adresse (Zusätzlich wird bei Systemtelefonen ein Link angezeigt, über den das WBM des Telefons geöffnet werden kann.)
- MAC-Adresse
- Aktuelle SW-Version
- HW-Version
- Status (Aktiviert/Deaktiviert)

Verbindungsaufbau-Status

Der Verbindungsaufbau-Status ermöglicht die Abfrage von Informationen über die bestehenden Verbindungen zu PSTN-Partnern (Public Switched Telephone Network-Partner, wie zum Beispiel öffentliche oder private Telekommunikations-netzte) des Kommunikationssystems OpenScape Business X.

ITSP-Status

Der ITSP-Status ermöglicht die Abfrage von Informationen über den aktuellen Status der vorkonfigurierten und eventuell hinzugefügten Internet-Telefonie-Service-Provider (ITSP). Angezeigt wird darüber hinaus, welche Teilnehmer für welchen ITSP eingerichtet wurden.

Die Status jedes ITSPs wird durch die Farbe des zugehörigen Rechtecks angezeigt (grün = OK, grau = nicht aktiviert/konfiguriert, orange = Mindestens ein Teilnehmer wurde nicht fehlerfrei eingerichtet.).

VPN-Status

Der VPN-Status ermöglicht die Abfrage von Informationen über die eingerichteten VPN-Tunnel des Kommunikationssystems OpenScape Business X.

Übersicht IP-Adressen

Angezeigt werden die im Kommunikationssystem OpenScape Business X konfigurierten IP-Adressen.

Darüber hinaus ist angegeben, über welchen Wizard und über welche Menüs im Experten-Modus die IP-Adressen konfiguriert werden können.

24.5.1.1 Wie Sie den Teilnehmer-Status abfragen

Mit dem Wizard **Status** können Sie den aktuellen Status aller eingerichteten Teilnehmer ermitteln.

Voraussetzungen

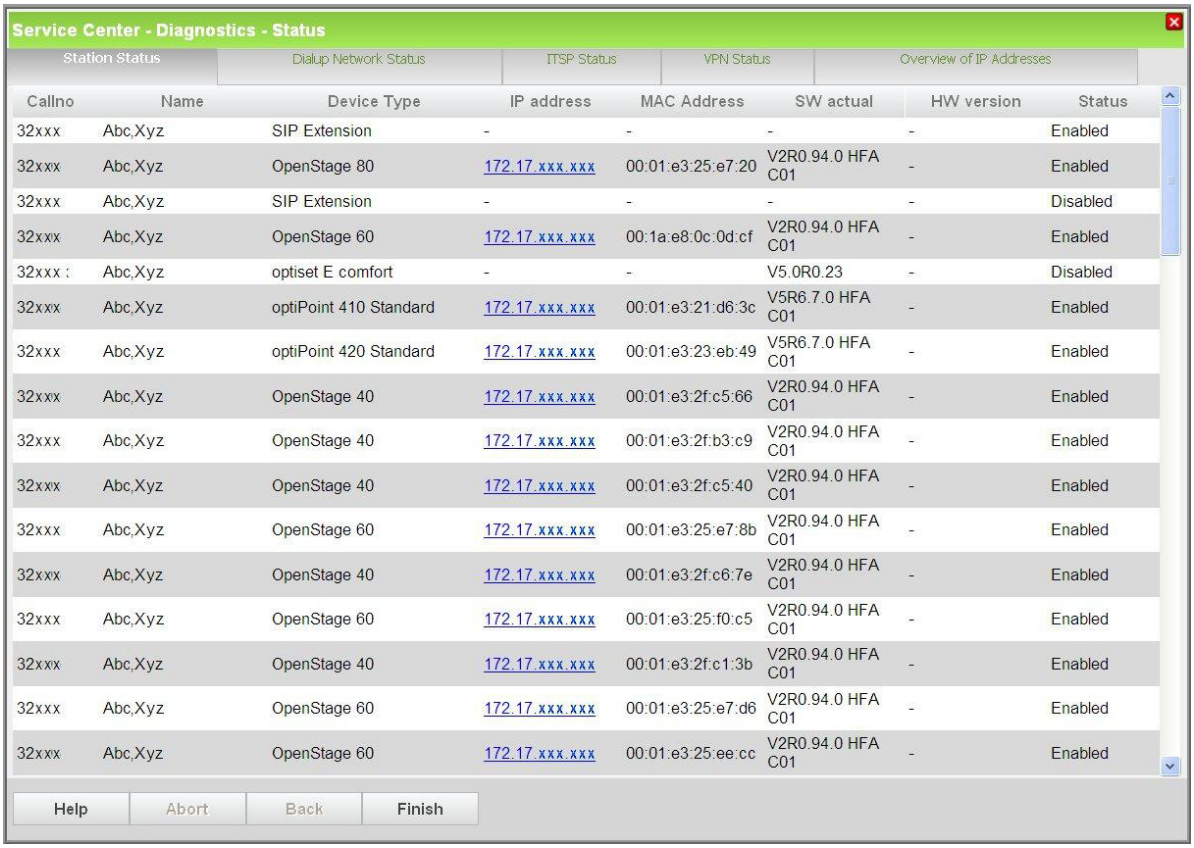
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Diagnose > Status**.

3) Klicken Sie auf die Registerkarte **Teilnehmer Status**. Es wird Ihnen der Status aller eingerichteten Teilnehmer angezeigt.



CallNo	Name	Device Type	IP address	MAC Address	SW actual	HW version	Status
32xxx	Abc,Xyz	SIP Extension	-	-	-	-	Enabled
32xxx	Abc,Xyz	OpenStage 80	172.17.xxx.xxx	00:01:e3:25:e7:20	V2R0.94.0 HFA C01	-	Enabled
32xxx	Abc,Xyz	SIP Extension	-	-	-	-	Disabled
32xxx	Abc,Xyz	OpenStage 60	172.17.xxx.xxx	00:1a:e8:0c:0d:cf	V2R0.94.0 HFA C01	-	Enabled
32xxx :	Abc,Xyz	optiset E comfort	-	-	V5.0R0.23	-	Disabled
32xxx	Abc,Xyz	optiPoint 410 Standard	172.17.xxx.xxx	00:01:e3:21:d6:3c	V5R6.7.0 HFA C01	-	Enabled
32xxx	Abc,Xyz	optiPoint 420 Standard	172.17.xxx.xxx	00:01:e3:23:eb:49	V5R6.7.0 HFA C01	-	Enabled
32xxx	Abc,Xyz	OpenStage 40	172.17.xxx.xxx	00:01:e3:2f:c5:66	V2R0.94.0 HFA C01	-	Enabled
32xxx	Abc,Xyz	OpenStage 40	172.17.xxx.xxx	00:01:e3:2f:b3:c9	V2R0.94.0 HFA C01	-	Enabled
32xxx	Abc,Xyz	OpenStage 40	172.17.xxx.xxx	00:01:e3:2f:c5:40	V2R0.94.0 HFA C01	-	Enabled
32xxx	Abc,Xyz	OpenStage 60	172.17.xxx.xxx	00:01:e3:25:e7:8b	V2R0.94.0 HFA C01	-	Enabled
32xxx	Abc,Xyz	OpenStage 40	172.17.xxx.xxx	00:01:e3:2f:c6:7e	V2R0.94.0 HFA C01	-	Enabled
32xxx	Abc,Xyz	OpenStage 60	172.17.xxx.xxx	00:01:e3:25:f0:c5	V2R0.94.0 HFA C01	-	Enabled
32xxx	Abc,Xyz	OpenStage 40	172.17.xxx.xxx	00:01:e3:2f:c1:3b	V2R0.94.0 HFA C01	-	Enabled
32xxx	Abc,Xyz	OpenStage 60	172.17.xxx.xxx	00:01:e3:25:e7:d6	V2R0.94.0 HFA C01	-	Enabled
32xxx	Abc,Xyz	OpenStage 60	172.17.xxx.xxx	00:01:e3:25:ee:cc	V2R0.94.0 HFA C01	-	Enabled

4) Klicken Sie auf **Beenden**.

24.5.1.2 Wie Sie den Verbindungsaufbau-Status abfragen

Mit dem Wizard **Status** können Sie den aktuellen Status der PSTN-Partner eines Kommunikationssystems OpenScape Business X ermitteln.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

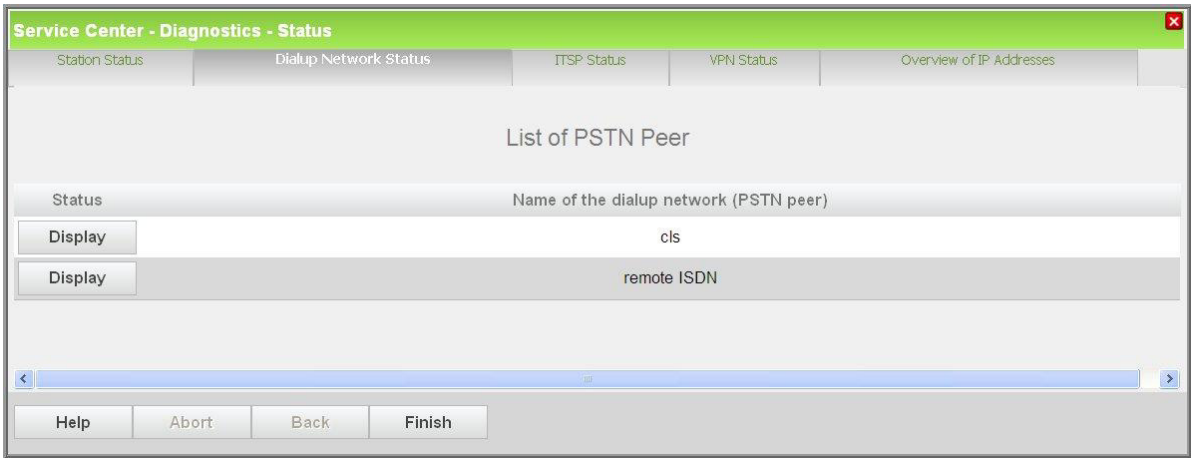
Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Diagnose > Status**.

3) Klicken Sie auf die Registerkarte **Status Verbindungsaufbau**. Es wird Ihnen die Liste der PSTN-Partner angezeigt.

4) Klicken Sie in der Zeile der gewünschten Verbindung (PSTN-Partner) auf **Anzeigen**. Es wird Ihnen der aktuelle Status dieser Verbindung (PSTN-Partner) angezeigt.



5) Wenn Sie die Statusinformationen einer weiteren Verbindung (PSTN-Partner) abrufen möchten, fahren Sie wie unter Schritt 3 beschrieben fort.

6) Klicken Sie auf **OK** und anschließend auf **Beenden**.

24.5.1.3 Wie Sie den ITSP-Status abfragen

Mit dem Wizard **Status** können Sie den aktuellen Status der Internet-Telefonie-Service-Provider (ITSP) ermitteln.

Voraussetzungen

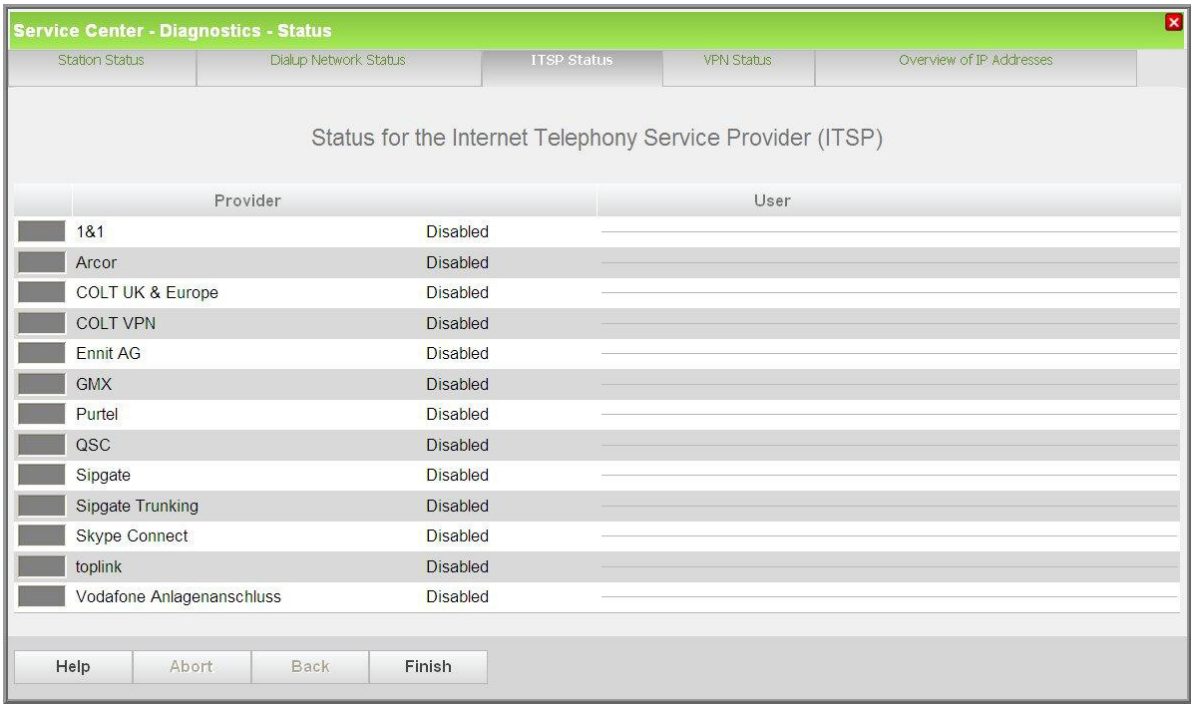
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Diagnose > Status**.

3) Klicken Sie auf die Registerkarte **ITSP Status**. Es wird Ihnen der aktuelle Status der vorkonfigurierten und eventuell hinzugefügten Internet-Telefonie-Service-Provider (ITSP) angezeigt.



4) Klicken Sie auf **Beenden**.

24.5.1.4 Wie Sie den VPN-Status abfragen

Mit dem Wizard **Status** können Sie den aktuellen Status aller eingerichteten VPN-Tunnel eines Kommunikationssystems OpenScape Business X ermitteln.

Voraussetzungen

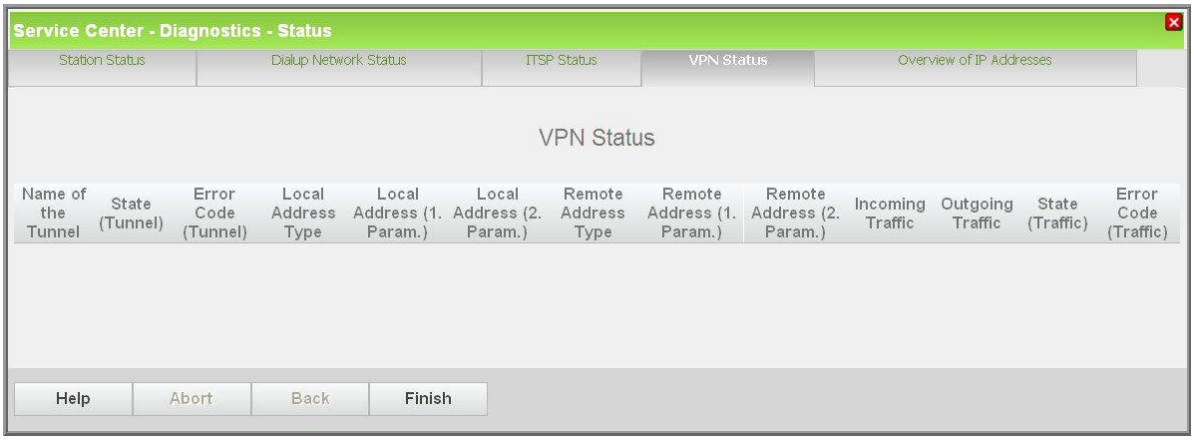
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Diagnose > Status**.

3) Klicken Sie auf die Registerkarte **VPN Status**. Es wird Ihnen der Status aller eingerichteten VPN-Tunnel angezeigt.



4) Klicken Sie auf **Beenden**.

24.5.1.5 Wie Sie IP-Adressen anzeigen

Mit dem Wizard **Status** können Sie eine Übersicht der in einem Kommunikationssystem OpenScape Business X konfigurierten IP-Adressen aufrufen. Darüber hinaus wird angezeigt, über welchen Wizard und über welche Menüs im Experten-Modus die IP-Adressen konfiguriert werden können.

Voraussetzungen

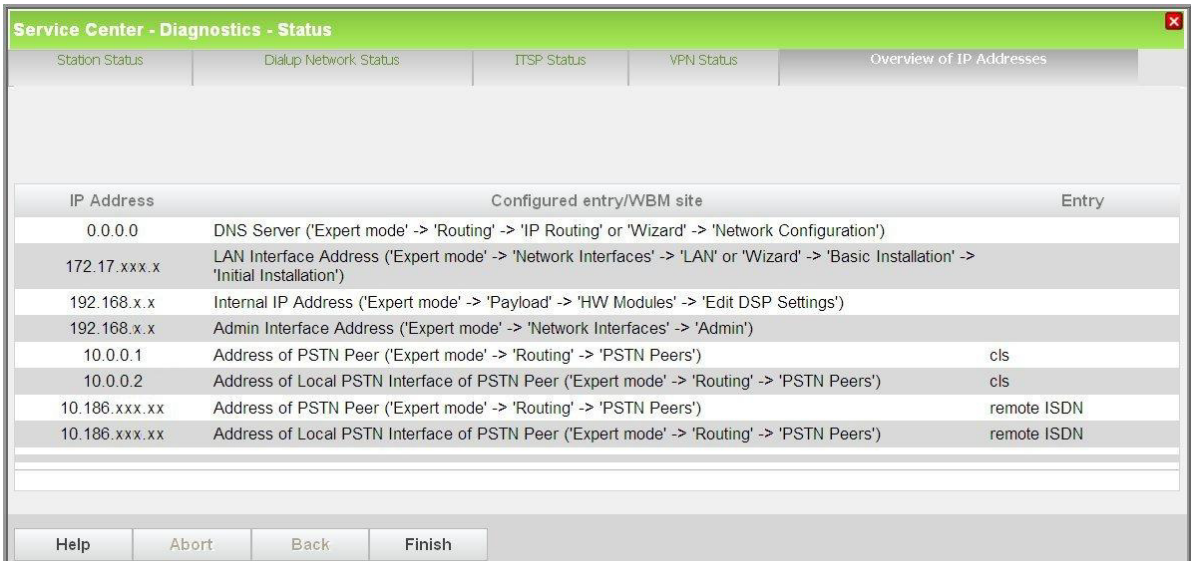
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Diagnose > Status**.

3) Klicken Sie auf die Registerkarte **Übersicht IP-Adressen**. Es wird Ihnen eine Übersicht der im Kommunikationssystem konfigurierten IP-Adressen angezeigt.



4) Klicken Sie auf **Beenden**.

24.5.2 Inventory

Anhand des Inventorys kann ein Administrator Informationen über die Hardware und Software von OpenScape Business X und über die Software von OpenScape Business S ermitteln.

OpenScape Business X

Der Abruf folgender Angaben ist möglich:

- Kommunikationssystem
  Unter anderem werden folgende Informationen angezeigt:
  - Grafische Darstellung des Kommunikationssystems und der Baugruppen
  - Sachnummer des Mainboards, MAC-Adresse, IP-Adresse, Host-Name, Version der Software
  - Angaben zum Speichervolumen, dem noch verfügbaren und dem belegten Speicher der SDHC-Karte.
  - Status aller Applikationen
- Baugruppen
  Unter anderem werden folgende Informationen angezeigt: Einbauplatz, Typ, Sachnummer und Status aller gesteckten Baugruppen.
- UC Booster Card (Application Board OCAB), falls vorhanden
  Unter anderem werden folgende Informationen angezeigt:
  - MAC-Adresse, IP-Adresse, Host-Name, Version der Software
  - Angaben zum Speichervolumen, dem noch verfügbaren und dem belegten Speicher der Festplatte.
  - Status aller Applikationen

Darüber hinaus kann die Zuordnung der Rufnummern zu den Baugruppen abgerufen werden.

OpenScape Business S

Der Abruf folgender Angaben ist möglich:

- Software
  Unter anderem werden folgende Informationen angezeigt: MAC-Adresse, IP-Adresse, Host-Name, Version der Software.
- Festplatten Information
  Angezeigt werden Angaben zum Speichervolumen, dem noch verfügbaren und dem belegten Speicher.
- Applikationen
  Angezeigt werden alle Applikationen und deren Status.

24.5.2.1 Wie Sie das Inventory von OpenScape Business X abfragen

Mit dem Wizard **Inventory** können Sie den aktuellen Status der Hardware und der Software der Kommunikationssysteme OpenScape Business X ermitteln.

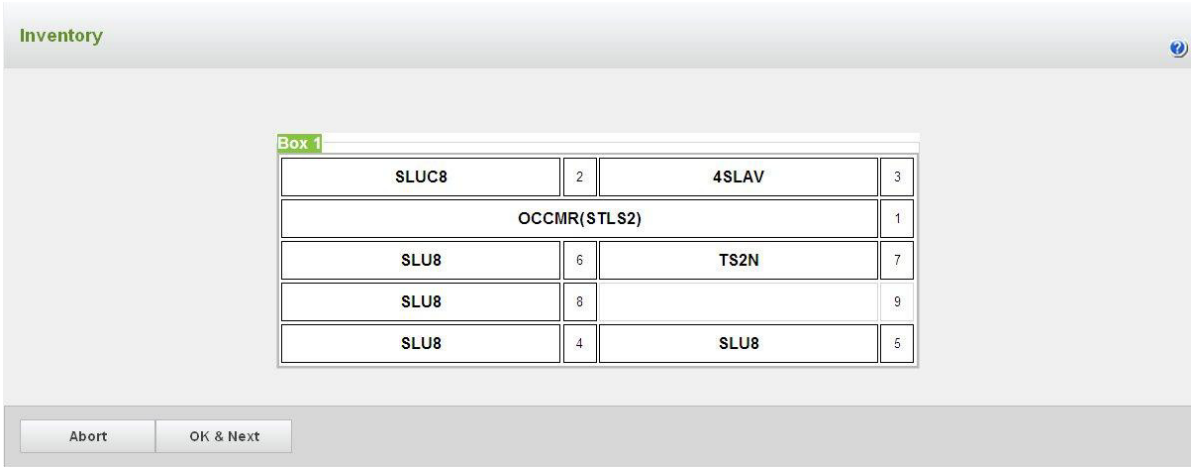
Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

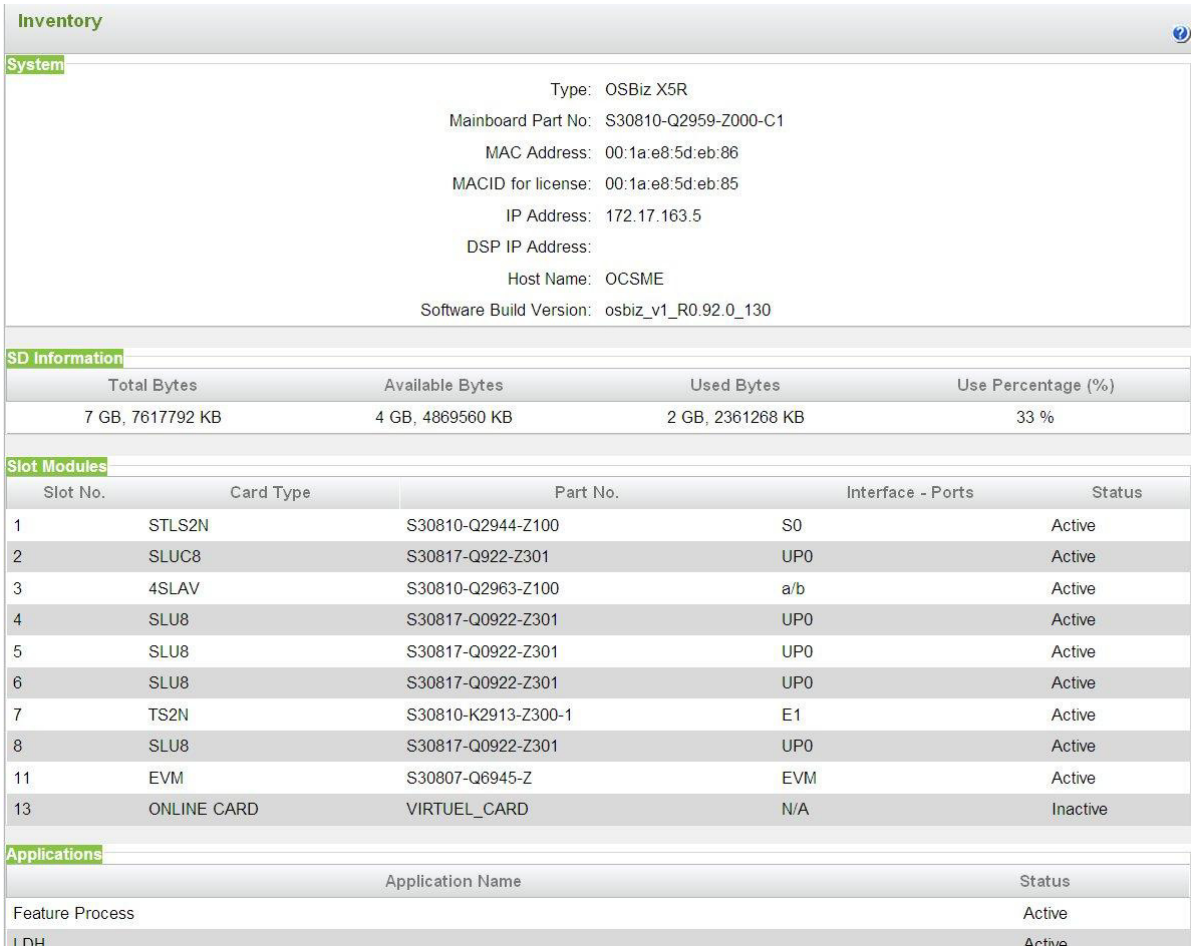
Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Inventory**. Es wird Ihnen eine grafische Darstellung des Kommunikationssystems und der Baugruppen angezeigt.



3) Klicken Sie auf **OK & Weiter**. Es werden Ihnen Informationen über das Kommunikationssystem, über den verfügbaren und den belegten Speicher der SDHC-Karte, über die Baugruppen und über den Applikationsstatus angezeigt.



Inventory

System

Type:	OSBiz X5R
Mainboard Part No:	S30810-Q2959-Z000-C1
MAC Address:	00:1a:e8:5d:eb:86
MACID for license:	00:1a:e8:5d:eb:85
IP Address:	172.17.163.5
DSP IP Address:	
Host Name:	OCSME
Software Build Version:	osbiz_v1_R0.92.0_130

SD Information

Total Bytes	Available Bytes	Used Bytes	Use Percentage (%)
7 GB, 7617792 KB	4 GB, 4869560 KB	2 GB, 2361268 KB	33 %

Slot Modules

Slot No.	Card Type	Part No.	Interface - Ports	Status
1	STLS2N	S30810-Q2944-Z100	S0	Active
2	SLUC8	S30817-Q922-Z301	UP0	Active
3	4SLAV	S30810-Q2963-Z100	a/b	Active
4	SLU8	S30817-Q0922-Z301	UP0	Active
5	SLU8	S30817-Q0922-Z301	UP0	Active
6	SLU8	S30817-Q0922-Z301	UP0	Active
7	TS2N	S30810-K2913-Z300-1	E1	Active
8	SLU8	S30817-Q0922-Z301	UP0	Active
11	EVM	S30807-Q6945-Z	EVM	Active
13	ONLINE CARD	VIRTUEL_CARD	N/A	Inactive

Applications

Application Name	Status
Feature Process	Active
LDH	Active

4) Klicken Sie auf **OK & Weiter**. Die anschließend angezeigten Informationen sind abhängig davon, ob das Kommunikationssystem mit einer UC Booster Card (Application Board OCAB) bestückt ist:

a) Ihr Kommunikationssystem ist nicht mit einer UC Booster Card bestückt: Es werden Ihnen Informationen über die Zuordnung der Rufnummern zu den Baugruppen angezeigt.

b) Ihr Kommunikationssystem ist mit einer UC Booster Card bestückt: Es werden Ihnen Informationen über die Baugruppe OCAB, über den verfügbaren und den belegten Speicher der Festplatte und über den Applikationsstatus angezeigt.

Klicken Sie auf **OK & Weiter**. Es werden Ihnen Informationen über die Zuordnung der Rufnummern zu den Baugruppen angezeigt.

5) Klicken Sie auf **Beenden**.

24.5.2.2 Wie Sie das Inventory von OpenScape Business S abfragen

Mit dem Wizard **Inventory** können Sie den aktuellen Status der Software von OpenScape Business S ermitteln.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Inventory**. Es werden Ihnen Informationen über die Software des Kommunikationssystems, über den verfügbaren und den belegten Speicher der Festplatten und über den Applikationsstatus angezeigt.

24.6 Automatische Aktionen

Über diese Funktion können einmalig oder regelmäßig durchzuführende Aktionen definiert werden. Diese Aktionen werden dann zum eingestellten Zeitpunkt automatisch durch das Kommunikationssystem ausgeführt.

24.6.1 Automatische Aktion Garbage Collection

Durch die automatische Aktion Garbage Collection kann regelmäßig eine automatische Speicherbereinigung auf dem Kommunikationssystem durchgeführt werden. Nach Abschluss jeder Speicherbereinigung führt das Kommunikationssystem einen Restart (Neustart) durch.

Bei der Darstellung im Menübaum kennzeichnet die Farbe des Listenpunkts den Status der Aktion (grün = Aktion aktiviert, rot = Aktion nicht aktiviert).

Durch Auswahl von **Aktion starten/stoppen** kann eine nicht aktive Aktion (roter Listenpunkt) aktiviert/gestartet und eine aktive Aktion (grüner Listenpunkt) deaktiviert/gestoppt werden.

In der Standardeinstellung ist die automatische Aktion Garbage Collection nicht aktiviert.

24.6.1.1 Wie Sie die automatische Aktion Garbage Collection ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

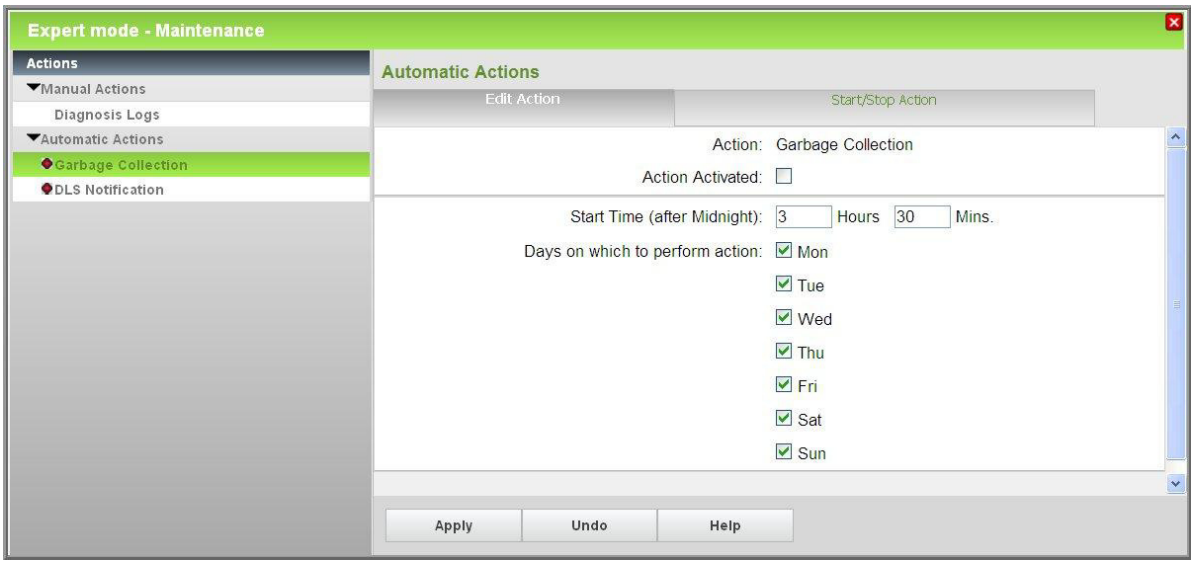
Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung > Aktionen**.

3) Klicken Sie im Menübaum auf **Aktionen > Automatische Aktionen > Garbage Collection**.

4) Klicken Sie auf die Registerkarte **Aktion ändern**.



5) Wählen Sie die gewünschte Einstellung aus:

- Wenn die Aktion Garbage Collection durchgeführt werden soll, aktivieren Sie das Kontrollkästchen **Aktion aktiviert**.
- Wenn die Aktion Garbage Collection nicht durchgeführt werden soll, deaktivieren Sie das Kontrollkästchen **Aktion aktiviert**.

6) Ändern Sie bei Bedarf den **Startzeitpunkt nach Mitternacht**.

Geben Sie im Feld **Std.** die Stunden und im Feld **Min.** die Minuten ein, nach deren Ablauf die Aktion gestartet werden soll.

Beispiel: Im Feld **Std.** wurde `3` und im Feld **Min.** `30` eingegeben. Das bedeutet, die Aktion Garbage Collection wird morgens um 3:30 Uhr durchgeführt.

7) Ändern Sie bei Bedarf die Wochentage über **Aktion an folgenden Wochentagen ausführen**.

Aktivieren Sie die Kontrollkästchen der Wochentage, an denen die Aktion durchgeführt werden soll. Deaktivieren Sie die Kontrollkästchen der Wochentage, an denen die Aktion nicht durchgeführt werden soll.

8) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.6.1.2 Wie Sie die automatische Aktion Garbage Collection starten (aktivieren)

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung > Aktionen**.

3) Klicken Sie im Menübaum auf **Aktionen > Automatische Aktionen**. Im Menübaum werden Ihnen die Namen aller automatischen Aktionen angezeigt. Nicht aktivierte Aktionen sind durch einen roten Listenpunkt gekennzeichnet. Aktivierte Aktionen sind durch einen grünen Listenpunkt gekennzeichnet.

4) Klicken Sie im Menübaum auf **Garbage Collection**.

5) Klicken Sie auf die Registerkarte **Aktion starten/stoppen**.

6) Klicken Sie auf **Start** und anschließend auf **OK**.

24.6.1.3 Wie Sie die automatische Aktion Garbage Collection stoppen (deaktivieren)

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung > Aktionen**.

3) Klicken Sie im Menübaum auf **Aktionen > Automatische Aktionen**. Im Menübaum werden Ihnen die Namen aller automatischen Aktionen angezeigt. Nicht aktivierte Aktionen sind durch einen roten Listenpunkt gekennzeichnet. Aktivierte Aktionen sind durch einen grünen Listenpunkt gekennzeichnet.

4) Klicken Sie im Menübaum auf **Garbage Collection**.

5) Klicken Sie auf die Registerkarte **Aktion starten/stoppen**.

6) Klicken Sie auf **Stop** und anschließend auf **OK**.

24.6.2 Automatische Aktion DLS Notification

Durch die automatische Aktion DLS Notification kann die automatische Anmeldung an einem externen DLS-Server beim Hochlauf des Kommunikationssystems initiiert werden.

Bei der Darstellung im Menübaum kennzeichnet die Farbe des Listenpunkts den Status der Aktion (grün = Aktion aktiviert, rot = Aktion nicht aktiviert).

Durch Auswahl von **Aktion starten/stoppen** kann eine nicht aktive Aktion (roter Listenpunkt) aktiviert/gestartet und eine aktive Aktion (grüner Listenpunkt) deaktiviert/gestoppt werden.

In der Standardeinstellung ist die automatische Aktion DLS Notification nicht aktiviert.

24.6.2.1 Wie Sie die automatische Aktion DLS Notification ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

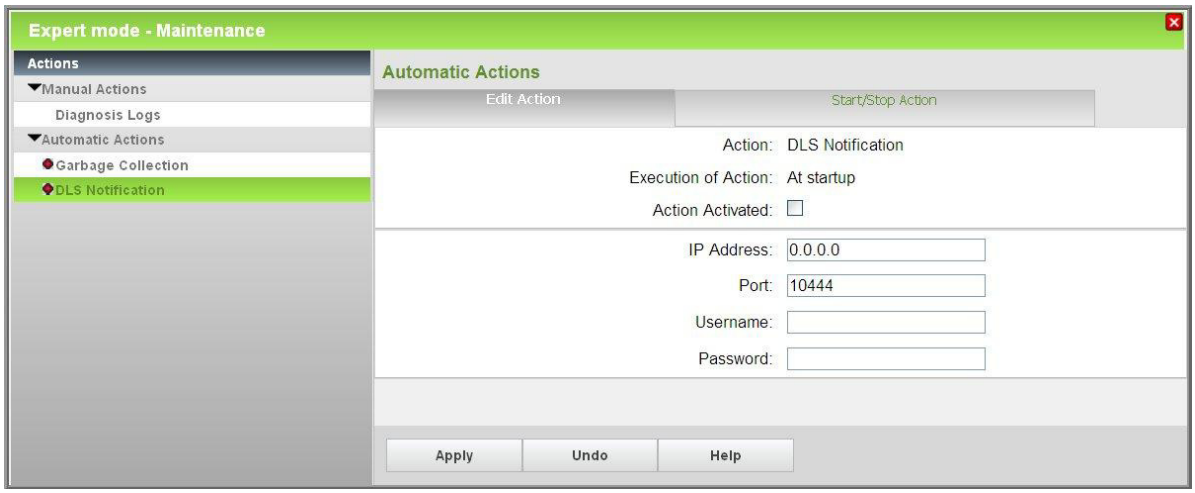
Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung > Aktionen**.

3) Klicken Sie im Menübaum auf **Aktionen > Automatische Aktionen > DLS Notification**.

4) Klicken Sie auf die Registerkarte **Aktion ändern**.



5) Wählen Sie die gewünschte Einstellung aus:

- Wenn die Aktion DLS Notification durchgeführt werden soll, aktivieren Sie das Kontrollkästchen **Aktion aktiviert**.
- Wenn die Aktion DLS Notification nicht durchgeführt werden soll, deaktivieren Sie das Kontrollkästchen **Aktion aktiviert**.

6) Ändern Sie bei Bedarf im Feld **IP-Adresse** die IP-Adresse des externen DLS-Servers.

7) Ändern Sie bei Bedarf im Feld **Port** den Port des externen DLS-Servers.

8) Ändern Sie bei Bedarf im Feld **Benutzername** den Benutzernamen für die Anmeldung am externen DLS-Server.

9) Ändern Sie bei Bedarf im Feld **Passwort** das Passwort für die Anmeldung am externen DLS-Server.

10) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.6.2.2 Wie Sie die automatische Aktion DLS Notification starten (aktivieren)

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung > Aktionen**.

3) Klicken Sie im Menübaum auf **Aktionen > Automatische Aktionen**. Im Menübaum werden Ihnen die Namen aller automatischen Aktionen angezeigt. Nicht aktivierte Aktionen sind durch einen roten Listenpunkt gekennzeichnet. Aktivierte Aktionen sind durch einen grünen Listenpunkt gekennzeichnet.

4) Klicken Sie im Menübaum auf **DLS Notification**.

5) Klicken Sie auf die Registerkarte **Aktion starten/stoppen**.

6) Klicken Sie auf **Start** und anschließend auf **OK**.

24.6.2.3 Wie Sie die automatische Aktion DLS Notification stoppen (deaktivieren)

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung > Aktionen**.

3) Klicken Sie im Menübaum auf **Aktionen > Automatische Aktionen**. Im Menübaum werden Ihnen die Namen aller automatischen Aktionen angezeigt. Nicht aktivierte Aktionen sind durch einen roten Listenpunkt gekennzeichnet. Aktivierte Aktionen sind durch einen grünen Listenpunkt gekennzeichnet.

4) Klicken Sie im Menübaum auf **DLS Notification**.

5) Klicken Sie auf die Registerkarte **Aktion starten/stoppen**.

6) Klicken Sie auf **Stop** und anschließend auf **OK**.

24.7 Power-Management

Das Power-Management versetzt das Kommunikationssystem abhängig von der Auslastung des Systems automatisch in einen Energiesparzustand. Dadurch wird der Energieverbrauch des Systems gesenkt und ein Beitrag zum Umweltschutz

geleistet. Die Zeitspanne, in der das System in den Energiesparzustand wechseln darf, ist einstellbar (z. B. nachts).

Das Power-Management kann nur aktiviert werden, wenn sich die LAN-Schnittstellen des Systems im Ethernet-Link-Modus **Auto** befinden. Im Energiesparzustand wechseln die LAN-Schnittstellen des Systems automatisch in den 100Mbit/s-Vollduplex-Modus. Die LAN-Schnittstellen der angeschlossenen Infrastruktur sollten sich ebenfalls im Autosense-Modus befinden.

Betriebszustände

- Aktivzustand (Active Mode)
  Im Aktivzustand werden Funktionen des Kommunikationssystem genutzt und es findet zwischen dem System und der angeschlossenen Infrastruktur signifikanter Datentransfer statt.
- Bereitschaftszustand (Idle Mode)
  Im Bereitschaftszustand werden kaum Funktionen des Kommunikationssystem genutzt und es findet zwischen dem System und der angeschlossenen Infrastruktur kein signifikanter Datentransfer statt. Wird eine Funktion eingeleitet, wechselt das System vom Bereitschaftszustand in den Aktivzustand.
- Energiesparzustand (Low Power Mode)
  Der Energiesparzustand hat gegenüber dem Bereitschaftszustand einen reduzierten Energiebedarf. Das System befindet sich im 100Mbit/s-Vollduplex-Modus.

Es besteht auch die Möglichkeit, das System permanent im Ethernet-Link-Modus 100Mbit/s-Vollduplex oder 100Mbit/s-Halbduplex zu betreiben.

24.7.1 Wie Sie das Power-Management aktivieren oder deaktivieren

Voraussetzungen

- Die LAN-Schnittstelle des Mainboards, über die das System an die LAN-Infrastruktur angeschlossen ist, befindet sich im Ethernet-Link-Modus **Auto**.
- Nur wenn eine UC Booster Card gesteckt ist: Die LAN-Schnittstelle der UC Booster Card, über die die UC Booster Card an die LAN-Infrastruktur angeschlossen ist, befindet sich im Ethernet-Link-Modus **Auto**.
- Die LAN-Schnittstellen der angeschlossenen Infrastruktur (z. B. IP-Telefone) befinden sich im Autosense-Modus.
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > Grundinstallation**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Power Management** zu starten.

4) Wenn Sie das Power-Management aktivieren möchten:

a) Aktivieren Sie das Kontrollkästchen **Power Management ein-/ ausschalten**.

b) Geben Sie unter **Beginn des LowPowerModes** und **Ende des LowPowerModes** die Zeitspanne an, in der das Kommunikationssystem in den Energiesparmodus wechseln soll.

5) Wenn Sie das Power-Management deaktivieren möchten, deaktivieren Sie das Kontrollkästchen **Power Management ein-/ausschalten**.

6) Klicken Sie auf **OK & Weiter**. Ihre Einstellungen werden übernommen.

7) Klicken Sie auf **Beenden**.

24.7.2 Wie Sie den Ethernet-Link-Modus der LAN-Schnittstellen ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Telefonie > Netzwerkschnittstellen**.

3) Wählen Sie den Ethernet-Link-Modus für die LAN-Schnittstelle des Mainboards aus:

a) Klicken Sie im Menübaum auf **Mainboard > LAN 2**. Über die LAN 2-Schnittstelle ist das System an die LAN-Infrastruktur angeschlossen.

b) Wenn Sie das Power-Management aktivieren wollen, wählen Sie in der Aufklappliste **Ethernet-Link-Modus** den Eintrag **Auto** aus.

c) Wenn Sie das System permanent in den Energiesparzustand setzen wollen, wählen Sie in der Aufklappliste **Ethernet-Link-Modus** den Eintrag **100HDX** oder **100FDX** aus.

INFO: Für die Ethernet-Link-Modi **100HDX**, **100FDX** und **1000FDX** kann das Power-Management kann nicht aktiviert werden.

---

d) Klicken Sie auf **Übernehmen**.

4) Nur falls eine UC Booster Card gesteckt ist: wählen Sie den Ethernet-Link-Modus für die LAN-Schnittstelle der UC Booster Card aus:

a) Klicken Sie im Menübaum auf **Application Board > LAN 2** oder **LAN 1**, je nachdem über welche LAN-Schnittstelle die UC Booster Card an die LAN-Infrastruktur angeschlossen ist (zu erkennen an dem Häkchen bei dem Kontrollkästchen **Schnittstelle aktiviert**).

b) Wenn Sie das Power-Management aktivieren wollen, wählen Sie in der Aufklappliste **Ethernet-Link-Modus** den Eintrag **Auto** aus.

c) Wenn Sie das System permanent in den Energiesparzustand setzen wollen, wählen Sie in der Aufklappliste **Ethernet-Link-Modus** den Eintrag **100HDX** oder **100FDX** aus.

INFO: Für die Ethernet-Link-Modi **100HDX**, **100FDX** und **1000FDX** kann das Power-Management kann nicht aktiviert werden.

---

d) Klicken Sie auf **Übernehmen**.

24.8 Überwachung und Wartung von OpenScape Business

OpenScape Business bietet verschiedene Funktionen, um den aktuellen Status des Systems zu überwachen und um Fehler zu finden und zu beheben.

24.8.1 Prüfen einer Netzwerkverbindung von OpenScape Business X

Durch eine ICMP (Internet Control Message Protocol)-Anforderung kann die Netzwerkverbindung zwischen einem Kommunikationssystem OpenScape Business X und der Ziel-Adresse mit Hilfe von Echoanforderungspaketen überprüft werden.

Echoanforderungspakete können sowohl über die Funktion **Ping** als auch über die Funktion **Traceroute** versendet werden. Die Antwortquittungen werden zusammen mit den Umlaufzeiten angezeigt.

Über die Funktion **Traceroute** werden die Echoanforderungspakete mit unterschiedlichen, ansteigenden TTL (Time-To-Live)-Werten gesendet.

24.8.1.1 Wie Sie Ping senden

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung > IP-Diagnose**.

3) Navigieren Sie im Menübaum zu **Mainboard > ICMP-Anforderung > Ping**.

4) Geben Sie im Feld **Ziel-Adresse** die IP-Adresse des gewünschten Ziels ein.

5) Geben Sie im Feld **Anzahl zu sendender Echoanforderungen** die gewünschte Anzahl ein (Standardwert = 3).

6) Klicken Sie auf **Senden**.

Anschließend werden Ihnen die Antwortquittungen zusammen mit den Umlaufzeiten angezeigt.

24.8.1.2 Wie Sie Traceroute testen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung > IP-Diagnose**.

3) Navigieren Sie im Menübaum zu **Mainboard > ICMP-Anforderung > Traceroute**.

4) Geben Sie im Feld **Ziel-Adresse** die IP-Adresse des gewünschten Ziels ein.

5) Geben Sie im Feld **TOS-Byte** den gewünschten Wert ein (Standardwert = 0).

6) Klicken Sie auf **Senden**.

Anschließend werden Ihnen die Antwortquittungen zusammen mit den Umlaufzeiten angezeigt.

24.8.2 SNMP (Simple Network Management Protocol)

Das Simple Network Management Protocol (SNMP) ist ein Netzwerkprotokoll, über das Netzwerkkomponenten (zum Beispiel Router, Server, Switches, Drucker, PC) von einer zentralen Station (Managementkonsole) aus überwacht und gesteuert werden können. Das Protokoll regelt hierbei die Kommunikation zwischen den überwachten Komponenten und der Überwachungsstation.

SNMP beschreibt den Aufbau der Datenpakete, die gesendet werden können, und den Kommunikationsablauf. SNMP wurde so ausgelegt, dass jedes netzwerkfähige Gerät in die Überwachung aufgenommen werden kann. Zu den Aufgaben des Netzwerkmanagements über SNMP gehören

- die Überwachung von Netzwerkkomponenten,
- die Fernsteuerung und Fernkonfiguration von Netzwerkkomponenten,
- die Fehlererkennung und Fehlerbenachrichtigung.

Zur Überwachung werden sogenannte Agenten eingesetzt. Dabei handelt es sich um Programme, die direkt auf den überwachten Komponenten laufen. Diese Programme sind in der Lage, den Zustand der Komponente zu erfassen und auch selber Einstellungen vorzunehmen oder Aktionen auszulösen. Mit Hilfe von

SNMP ist es möglich, dass die zentrale Managementkonsole mit den Agenten über ein Netzwerk kommunizieren kann.

> ***INFO:*** OpenScape Business unterstützt SNMPv2c, reagiert aber auch auf SNMPv1 snmpget Anfragen.

Management-Informationsdatenbanken MIB

Der Umfang der Daten, die über SNMP verwaltet werden können, wird in Management-Informationsdatenbanken (MIBs) festgelegt. MIBs sind Datenmodelle, die zu verwaltende Netzwerkkomponenten in vorgegebener Weise beschreiben. Die MIB der Kommunikationssysteme OpenScape Business X kann über das WBM (Service-Center) heruntergeladen werden.

Die Kommunikationssysteme verfügen über einen eigenen SNMP-Agenten, der den Zugriff auf eine Reihe von Systemdaten ermöglicht, die in seiner Management-Informationsdatenbank MIB gespeichert sind. Die MIB liefert grundlegende Systeminformationen, Statusinformationen, ereignisbezogene Daten sowie Informationen zu installierter Hardware (Slots) und eingerichteten Verbindungen (Ports).

SNMP ermöglicht die zentrale Überwachung und Administration der Netzwerkkomponenten - inklusive der Kommunikationssysteme selbst. Möglich ist damit

- das Ansprechen eines Kommunikationssystems über TCP/IP.
- der Datenzugriff über externe Management-Applikationen.
- die Realisierung von Fernwartungsaufgaben.
- die Visualisierung des Betriebszustands des Kommunikationssystems.
- die Übermittlung servicerelevanter Fehler. (Traps).

Communities

Der Zugriff auf die SNMP-Daten (MIBs) wird durch Communities geregelt. Dabei wird zwischen der lesenden, schreibenden und der Trap-Community unterschieden. Hinter einer Community verbirgt sich jeweils eine IP-Adresse.

Um zum Beispiel einem PC den lesenden Zugriff auf die SNMP-Daten (MIBs) zu ermöglichen, muss die IP-Adresse dieses PCs in die Liste der lesenden Communities eingetragen werden. Um lesenden und schreibenden Zugriff zu erhalten, muss die IP-Adresse in die Liste der schreibenden Communities eingetragen werden.

Über Trap-Communities werden die Empfänger von Fehlermeldungen (Traps) verwaltet.

Traps

Bei Problemen eines Kommunikationssystems werden Traps erzeugt, um über Fehler und Ausfälle zu informieren. Es gibt folgende Arten von Traps:

- System-Traps = Systemfehler, die sofortige Maßnahmen zur Behebung erfordern.
- Leistungs-Traps = Informationen zu Leistungsproblemen, die jedoch keine Behebung erfordern.

Traps sind nach ihrer Auswirkung klassifiziert und können durch einen Administrator mit dem Profil **Expert** über das WBM abgerufen werden. Angezeigt wird eine Liste aller empfangenen Traps mit folgenden Informationen:

Tabellenspalte	Bedeutung
VarBind1 (Severity)	Auswirkungsklasse des Traps Folgende Einträge sind möglich: Critical: Fehlermeldung. Der Fehler hat problematische Auswirkungen. Major: Fehlermeldung. Der Fehler kann problematische Auswirkungen haben. Minor: Fehlermeldung. Der Fehler hat keine problematischen Auswirkungen. Warning: Meldung über einen möglicherweise problematischen Vorgang oder Zustand, jedoch keine Fehlermeldung. Deleted Information: Reine Statusmeldung, keine Fehlermeldung. Intermediate status Other traps
VarBind2 (Name)	Name des Traps
Generischer Name	Allgemeine Bezeichnung, wie zum Beispiel Enterprise Specific
Spezifischer Name	Typ des Traps (1 = Software, 2 = Hardware)
Enterprise	–
Zeit	Zeitpunkt des Fehlers
Index	Listennummer

Die Anzeige der Traps wird alle 30 Sekunden aktualisiert. Die Sortierung der Traps erfolgt in der Reihenfolge ihres Auftretens.

Durch Klicken auf einen Trap-Namen werden die Detaildaten des Traps angezeigt.

24.8.2.1 Wie Sie alle Communities anzeigen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung > SNMP**.

3) Klicken Sie im Menübaum auf **SNMP > Communities**. Es wird Ihnen eine Liste aller Communities mit den zugehörigen Daten (IP-Adresse, Community, Typ) angezeigt.



24.8.2.2 Wie Sie eine Community hinzufügen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung > SNMP**.

3) Wählen Sie die gewünschte Community aus:

- Wenn Sie eine lesende Community hinzufügen möchten, klicken Sie im Menübaum auf **SNMP > Communities > Lesende Communities**. Klicken Sie auf die Registerkarte **Lesende Community hinzufügen**.
- Wenn Sie eine schreibende Community hinzufügen möchten, klicken Sie im Menübaum auf **SNMP > Communities > Schreibende Communities**. Klicken Sie auf die Registerkarte **Schreibende Community hinzufügen**.
- Wenn Sie eine Trap-Community hinzufügen möchten, klicken Sie im Menübaum auf **SNMP > Communities > Trap Communities**. Klicken Sie auf die Registerkarte **Trap Community hinzufügen**.

4) Geben Sie im Feld **IP-Adresse** die IP-Adresse der neuen Community ein.

5) Geben Sie im Feld **Community** den Namen der neuen Community ein.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.8.2.3 Wie Sie eine Community ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung > SNMP**.
3) Navigieren Sie im Menübaum unter **SNMP > Communities > ...** zur gewünschten Community.
4) Klicken Sie auf die Registerkarte **Community ändern**.
5) Ändern Sie die Community.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.8.2.4 Wie Sie eine Community löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung > SNMP**.
3) Navigieren Sie im Menübaum unter **SNMP > Communities > ...** zur gewünschten Community.
4) Klicken Sie auf die Registerkarte **Community löschen**.
5) Klicken Sie auf **Löschen** und anschließend auf **OK**.

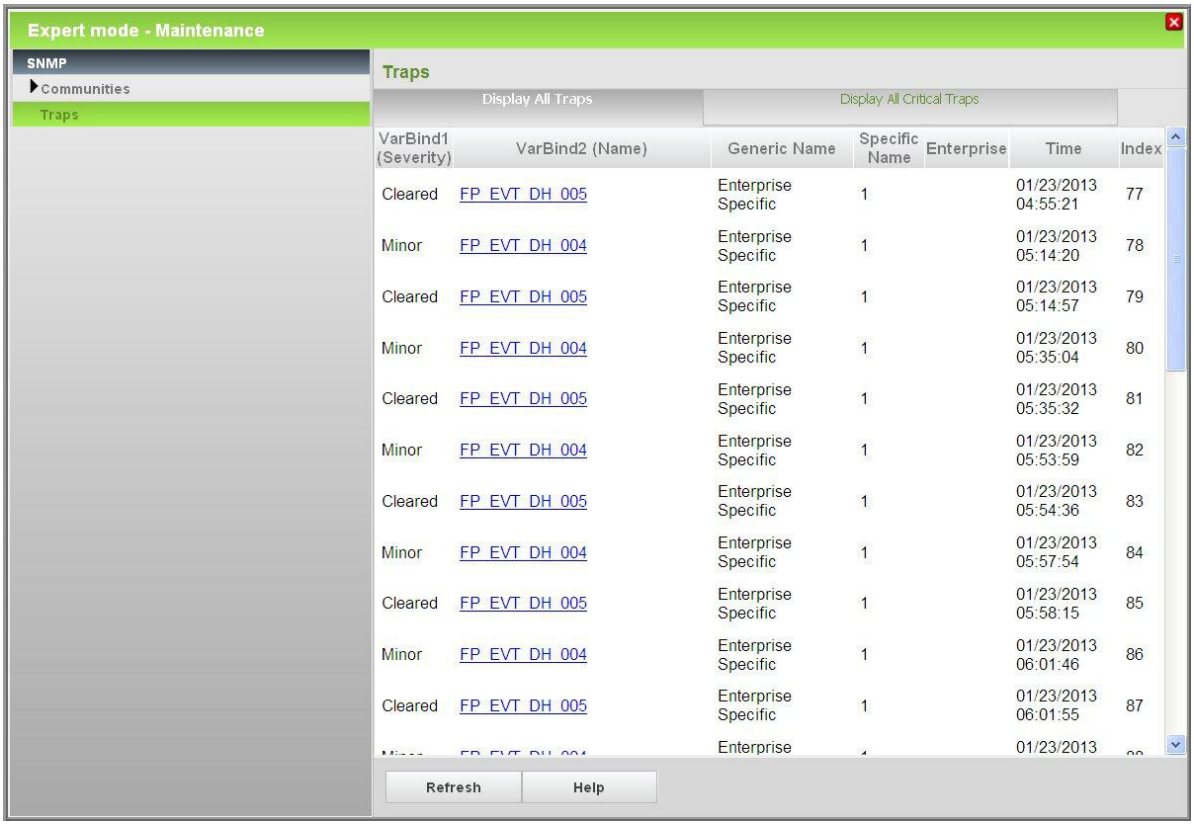
24.8.2.5 Wie Sie Traps anzeigen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung > SNMP**.
3) Klicken Sie im Menübaum auf **SNMP > Traps**.
4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn die Liste aller Traps angezeigt werden soll, klicken Sie auf die Registerkarte **Alle Traps anzeigen**.



- Wenn die Liste aller kritischen Traps angezeigt werden soll, klicken Sie auf die Registerkarte **Alle kritischen Traps anzeigen**.

24.8.2.6 Wie Sie Details eines Traps anzeigen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung > SNMP**.

3) Klicken Sie im Menübaum auf **SNMP > Traps**.

4) Klicken Sie auf die Registerkarte **Alle Traps anzeigen**. Es wird Ihnen eine Liste aller Traps mit den zugehörigen Daten angezeigt.

5) Klicken Sie auf den Namen des gewünschten Traps. Es werden Ihnen die Detaildaten dieses Traps angezeigt.

6) Klicken Sie auf die Registerkarte **Alle Traps anzeigen**, um die Liste aller Traps wieder aufzurufen.

24.8.3 Manuelle Aktionen

Durch manuelle Aktionen können verschiedene Protokolldaten (Diagnosedaten / Diagnose-Protokolle) geladen werden.

Ein Administrator mit dem Profil **Advanced** kann über den Wizard **Trace** Diagnosedaten (Diagnose-Protokolle) laden.

Ein Administrator mit dem Profil **Expert** kann über den **Experten-Modus** Diagnose-Protokolle laden.

Folgende Protokolle können geladen werden:

Protokoll	Erläuterung	Anwendungsfall
Trace-Protokoll	Standard-Trace-Datei, wenn Trace-Profile aktiviert werden. Zwischen folgenden Optionen kann gewählt werden: • **Gesamtes Protokoll**: Die gesamten vorhandenen Systemtrace-Protokolldateien werden heruntergeladen. • **Protokoll von heute**: Die Systemtrace-Protokolldateien des heutigen Tages (ab 00:00 Uhr) werden heruntergeladen. • **Eigene Auswahl**: **Von:** XXX **Bis:** YYY: Die Systemtrace-Protokolldateien des ausgewählten Zeitraums werden heruntergeladen.	Keine spezielle Anwendung
Event-Protokoll	Aktionen/Events des Kommunikationssystems (Reset, Ein-/Ausschalten usw.)	Keine spezielle Anwendung
Admin-Protokoll	Meldungen über Administrationsvorgänge am Kommunikationssystem (Login-Versuche usw.)	Keine spezielle Anwendung
Lizenz-Protokolle	Meldungen über lizenzierungspflichtige Komponenten des Kommunikationssystems	Probleme bei der Lizenzierung (Lizenzdatei kann nicht aktiviert werden usw.)
Kunden-Trace	Meldungen für den Kunden-Trace werden in ausführlicherer Form dargestellt, als zum Beispiel im Trace-Protokoll (Remote-Login, ITSP-Login usw.).	Probleme mit der ITSP (Internet Telefonie Service Provider)-Anbindung oder beim Remote-Login
Framework-Protokoll	Meldungen des WBM	Probleme bei der Lizenzierung, beim Sichern (Backup), beim Wiederherstellen (Restore) oder mit dem WBM
Diagnose-Protokoll	Diagnose Logs des Kommunikationssystems (FP/LDH)	Absturz oder unkontrolliertes Herunterfahren des Kommunikationssystems

Protokoll	Erläuterung	Anwendungsfall
UC Suite-Protokolle	Meldungen der UC Suite des Kommunikationssystems (UC Suite-, CSP- und MEB-Protokolle) Zwischen folgenden Optionen kann gewählt werden: • **Gesamtes Protokoll**: Alle vorhandenen UC Suite-, CSP- und MEB-Protokolldateien werden heruntergeladen. • **Protokoll von heute**: Die UC Suite-, CSP- und MEB-Protokolldateien des heutigen Tages (ab 00:00 Uhr) werden heruntergeladen. • **Eigene Auswahl**: **Von:** XXX **Bis:** YYY: Die UC Suite-, CSP- und MEB-Protokolldateien des ausgewählten Zeitraums werden heruntergeladen. Alle Protokolldateien werden in einer komprimierten Datei zusammengefasst. Für die OpenScape Business-Protokolle gelten folgende Dateibezeichnungen: UC Suite-Protokolldateien = `vs_jjjj_mm_tt.log`, CSP-Protokolldateien = `csptrace_jjjj_mm_tt.log`, MEB-Protokolldateien = `mebtrace_jjjj_mm_tt.log`. ***INFO***: Diagnosedaten können nur beim Betrieb mit UC Booster Card OCAB heruntergeladen werden. Bei Einsatz des OpenScape Business UC Booster Servers müssen Diagnosedaten über den Server selbst heruntergeladen werden.	Probleme mit der UC Suite und/oder den Clients (myPortal for Desktop, myAttendant usw.)
Applikationsprotokolle	Meldungen des Applikationsanteils des Kommunikationssystems (zum Beispiel CSP-Protokolle) Ein Administrator mit dem Profil **Expert** kann über den **Experten-Modus** zwischen folgenden Optionen wählen: • **Gesamtes Protokoll**: Alle vorhandenen Protokolldateien werden heruntergeladen • **Protokoll von heute**: Die Protokolldateien des heutigen Tages (ab 00:00 Uhr) werden heruntergeladen. • **Eigene Auswahl**: **Von:** XXX **Bis:** YYY: Die Protokolldateien des ausgewählten Zeitraums werden heruntergeladen. Alle Protokolldateien werden in einer komprimierten Datei zusammengefasst.	Probleme mit dem Applikationsanteil des Kommunikationssystems
System-Diagnose-Protokolle	Diagnose Logs des Kommunikationssystems	Keine spezielle Anwendung
PPP-Protokoll	Meldungen zum Point-to-Point-Protokoll	Probleme bei Einwahl (Dial-In)- oder Auswahl (Dial-Out)-Verbindungen
CoreLog-Protokoll	CoreLogs werden bei Resets usw. erstellt (wie Memory Dumps bei einem PC).	Absturz oder unkontrolliertes Herunterfahren von OpenScape Business

Nach Auswahl der gewünschten Protokolle wird eine komprimierte Datei erzeugt und in einem anzugebenden Verzeichnis gespeichert.

24.8.3.1 Wie Sie Diagnosedaten / Diagnose-Protokolle herunterladen

Mit dem Wizard **Trace** können Sie Diagnosedaten (Diagnose-Protokolle) der Kommunikationssysteme herunterladen.

Voraussetzungen

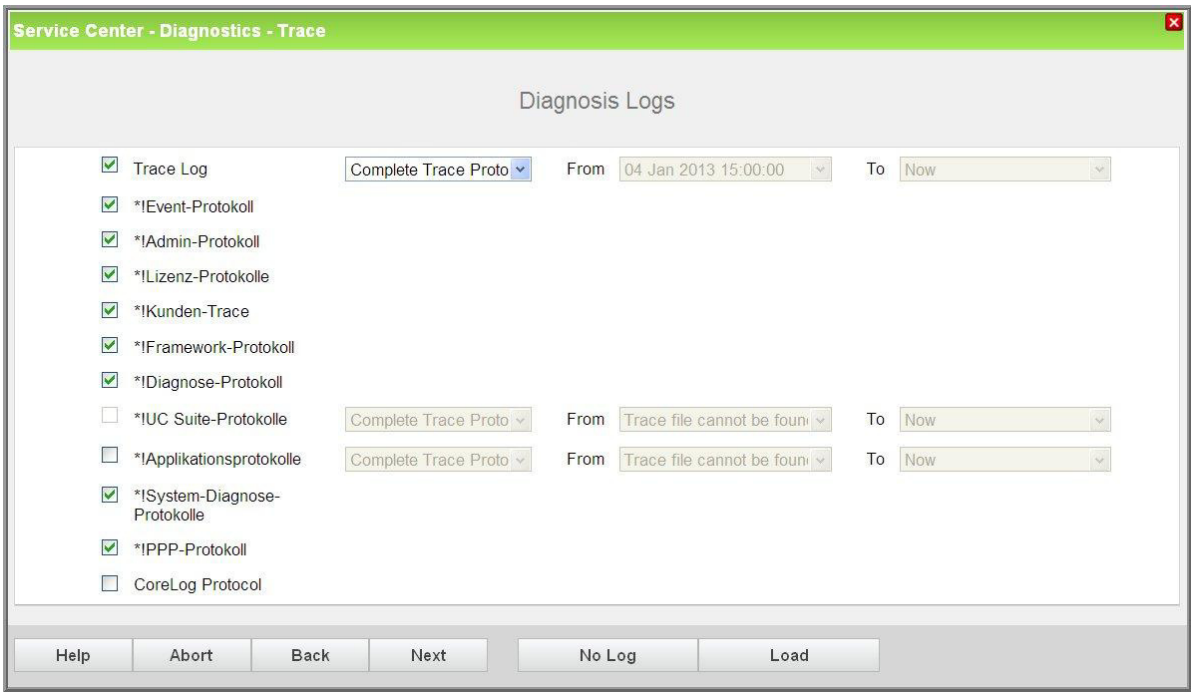
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Diagnose > Trace**.

3) Klicken Sie auf **Diagnosedaten**.



4) Aktivieren Sie die Kontrollkästchen der Protokolle, die Sie herunterladen wollen. Deaktivieren Sie die Kontrollkästchen der Protokolle, die Sie nicht herunterladen wollen.

5) Klicken Sie auf **Laden** und anschließend auf **OK**. Es erscheint das Dateidownload-Fenster.

6) Speichern Sie die Datei im gewünschten Verzeichnis. Schließen Sie anschließend das Fenster, das den Download der Datei bestätigt.

7) Klicken Sie auf **Weiter** und anschließend auf **Beenden**.

24.8.4 Traces

Anhand von Traces können Programmschritte und ihre Resultate während eines Programmablaufs aufgezeichnet werden. In Verbindung mit weiteren Diagnosedaten kann damit ein fehlerhaftes Programm bis zur Fehlerursache zurückverfolgt werden. Über die Trace-Profile und Trace-Komponenten wird konfiguriert, welche Traces in welcher Detailtiefe aufgezeichnet werden.

INFO: Das Aktivieren von Traces wirkt sich negativ auf die System-Performance aus und darf nur durch erfahrene Administratoren und nur in Absprache mit dem zuständigen Service-Support erfolgen.

Insbesondere der Konsolen-Trace belegt wesentliche System-Ressourcen und beeinträchtigt dadurch die Leistung des Kommunikationssystems.

Vernetzung

Für die Diagnose von vernetzten Kommunikationssystemen müssen die Trace-Daten jedes einzelnen Knotens separat erfasst werden. Die zentrale Erfassung von Trace-Daten vernetzter Kommunikationssysteme ist nicht möglich.

Trace-Format-Konfiguration

Über die Funktion Trace-Format-Konfiguration kann ein Administrator mit dem Profil **Expert** definieren, welche Header-Daten in der Trace-Ausgabe enthalten sein sollen und wie die Trace-Daten formatiert werden sollen.

Header-Daten für die Trace-Ausgabe (In der Standardeinstellung sind alle Optionen aktiviert.):

- Globale Trace-Header Format-Einstellungen
  Ist diese Option aktiviert, können die Optionen für die folgenden Header-Daten aktiviert oder deaktiviert werden.
- Subsystem-ID
- Task-Name
- Task-ID
- Zeit
- Modul-Name
- Zeilennummer

Aufbereitung der Trace-Daten (Formatierung):

- Volle Formatierung mit Parameterexpansion (Standard) = großes Datenvolumen, normale Trace-Performance. Standardeinstellung
- Eingeschränkt (Meldungstypen binär, speziell für X-Tracer) = mittleres Datenvolumen, schnelle Trace-Performance.
- Eingeschränkt (nur Expansion elementarer Datentypen) = geringes Datenvolumen, sehr schnelle Trace-Performance.

- Performanceoptimierter Trace ohne Parameterexpansion = sehr geringes Datenvolumen, extrem schnelle Trace-Performance.

> ***INFO:*** Zu beachten ist, dass zusätzliche Trace-Header-Daten und eine umfangreichere Trace-Daten-Formatierung die Gesamt-Performance eines Traces reduzieren.

Trace-Ausgabe-Interfaces

Über diese Funktion kann ein Administrator mit dem Profil **Expert** die Schnittstellen für die Trace-Ausgabe definieren. Möglich ist entweder die Aktivierung des Datei-Trace oder des Trace über LAN oder die Deaktivierung beider Schnittstellen.

Trace-Ausgabe-Interface	Erläuterung	Standardeinstellung
Datei-Trace	**Datei-Trace aktivieren** Trace-Meldungen werden im Kommunikationssystem in eine Protokolldatei eingetragen. Bei aktivierter Option gelten folgende Einstellungen: **Max. Trace-Quota (kByte):** Anzeige der maximalen Größe des Trace-Speichers **Strategie bei Erreichen der max. Quota**. Ausgewählt werden kann zwischen **Wrap Around (Lösche älteste Datei)** und **Datei-Trace wird temporär gestoppt**. **Zeit, nach der jeweils eine neue Trace-Datei angelegt wird (s):** 900 **Zeitraum, für den Trace-Dateien verfügbar sind:** Angegeben ist der aktuelle Zeitraum.	Aktiviert
Trace über LAN	**Trace über LAN aktivieren** Trace-Meldungen werden über die LAN-Schnittstelle übertragen. Bei aktivierter Option gilt folgende Einstellung: **Timer-Wert** = 25 s (Verzögerungszeit, bis Daten übertragen werden.)	Nicht aktiviert

Trace-Protokoll

Ist das Trace-Ausgabe-Interface Datei-Trace aktiviert, kann ein Administrator mit dem Profil **Expert** die resultierenden Protokolldateien über diese Funktion auf einen PC übertragen oder löschen.

Digitale Prüfschleife

Digitale Prüfschleifen werden zur Leitungsüberprüfung von B-Kanälen der S_0-, S_{2M}- und T1-Schnittstellen eventuell vorhandener Baugruppen eingesetzt. Die

Aktivierung digitaler Prüfschleifen sollte nur nach Aufforderung durch den Service-Provider erfolgen.

Die Konfiguration von digitalen Prüfschleifen ist ausschließlich mit Manager E möglich.

Event Viewer / Kunden-Trace-Protokoll

Ein Administrator mit dem Profil **Advanced** kann über den Wizard **Event Viewer** die Ereignis-Anzeige (Kunden-Trace) starten. Darüber hinaus kann die Kunden-Trace-Protokolldatei auf einen PC übertragen oder gelöscht werden.

Beschrieben ist die Vorgehensweise für folgende Funktionen, die über den Wizard gestartet werden können:

- *Wie Sie das Event Viewer-Protokoll / Kunden-Trace-Protokoll anzeigen oder ändern*
- *Wie Sie das Event Viewer-Protokoll / Kunden-Trace-Protokoll herunterladen oder öffnen*
- *Wie Sie das Event Viewer-Protokoll / Kunden-Trace-Protokoll löschen*

Ein Administrator mit dem Profil **Expert** kann über den **Experten-Modus** die Anzeige der Kunden-Trace-Protokolldatei starten. Darüber hinaus kann die Kunden-Trace-Protokolldatei auf einen PC übertragen oder gelöscht werden.

M5T-Trace-Komponenten

Diese Funktion dient zur Überwachung des SIP-Stacks durch einen Administrator mit dem Profil **Expert**. Für jede M5T-Trace-Komponente kann die Detailtiefe der Aufzeichnung über Trace-Levels (0 = geringste Detailtiefe bis 4 = größte Detailtiefe) definiert werden.

Secure Trace

Diese Funktion dient zur Aufzeichnung von verschlüsselten VoIP-Nutz- und Signalisierungsdatenströmen durch einen Administrator mit dem Profil **Expert**.

Bei aktiviertem Leistungsmerkmal Signaling and Payload Encryption (SPE) werden VoIP-Nutz- und Signalisierungsdatenströme vom und zum Kommunikationssystem und zwischen IP-Telefonen verschlüsselt.

Um im Fehlerfall eine Analyse zu gewährleisten, können für einen begrenzten Zeitraum zusätzliche Trace-Informationen (**Secure Trace**) im LAN übertragen werden. Dabei werden asymmetrisch verschlüsselte Secure-Trace-Dateien erzeugt, deren Entschlüsselung und Analyse nur durch die Entwicklung möglich ist.

Um die Nutzung der Secure-Trace-Funktion einzuschränken, wurden folgende Sicherheitsmerkmale implementiert:

- Ein Servicetechniker muss einen sogenannten öffentlichen Schlüssel (Zertifikat) in das betroffene Kommunikationssystem importieren. Das Zertifikat ist Teil einer X.509-Datei und Voraussetzung dafür, dass ein Secure Trace erzeugt werden kann. Die X.509-Datei wird durch die Entwicklung bereitgestellt. Das enthaltene Zertifikat ist maximal einen Monat gültig.

- Das Starten und Stoppen des Secure Trace ist durch ein besonderes Passwort (Passphrase) geschützt. Dieses Passwort ist nur dem Kunden bekannt.

Somit ist das Zertifikat der Schlüssel des Servicetechnikers und das Passwort (Passphrase) der Schlüssel des Kunden. Beide Schlüssel sind notwendig, um die Secure-Trace-Funktion zu aktivieren.

Ablauf für die Erzeugung eines Secure Trace:

1. Ein Servicetechniker stellt ein Problem im Kunden-LAN fest. Zusammen mit der zuständigen Entwicklung wird die Notwendigkeit erkannt, einen Secure Trace zu erzeugen.
2. Der Kunde wird über die Notwendigkeit informiert und muss bestätigen, dass er informiert wurde. Anschließend gibt der Kunde eine Bestellung zur Erzeugung eines Secure Trace auf, in der Datum und Uhrzeit des Beginns und des Endes der Überwachung genannt werden.
3. Ein Entwickler erstellt ein Schlüsselpaar, das aus dem öffentlichen Schlüssel und dem privaten Schlüssel besteht. Mit diesem Schlüsselpaar kann nur ein einziger Secure Trace erzeugt werden. Die Zertifikate werden folgendermaßen verwendet
   - Das Zertifikat mit dem privaten Schlüssel ist streng geheim und kann nur von autorisierten Entwicklern benutzt werden.
     Der private Schlüssel ist zur Entschlüsselung der Secure-Trace-Dateien erforderlich.
   - Das Zertifikat mit dem öffentlichen Schlüssel wird dem Servicetechniker in Form einer X.509-Datei im PEM- oder im Binärformat übergeben.
     Der Import dieses Zertifikats in das betroffene Kommunikationssystem ist Voraussetzung dafür, dass ein Secure Trace erzeugt werden kann.
4. Der Servicetechniker informiert den Kunden über den bevorstehenden Beginn der Secure-Trace-Erzeugung. Der Kunde muss die betroffenen Teilnehmer informieren.

   HINWEIS: Das Aufzeichnen von Gesprächen und Verbindungsdaten ist ein Strafttatbestand, falls die betroffenen Teilnehmer nicht darüber informiert wurden.

5. Der Servicetechniker importiert das Zertifikat mit dem öffentlichen Schlüssel in das betroffene Kommunikationssystem.
6. Der Kunde startet den Secure Trace durch Eingabe des Passworts (Passphrase). Die Secure-Trace-Dateien werden erzeugt.
   Start und der Stopp des Secure Trace werden durch das Kommunikationssystem protokolliert.
7. Nach Abschluss der Secure-Trace-Erzeugung wird der Kunde über das Ende der Secure-Trace-Aktivitäten informiert. Der Servicetechniker entfernt das Zertifikat vom Kommunikationssystem.
8. Die Secure-Trace-Dateien werden der Entwicklung zur Verfügung gestellt.
9. Ein Entwickler entschlüsselt den Secure-Trace-Dateien mit Hilfe des privaten Schlüssels. Anschließend erfolgt die Analyse der entschlüsselten Daten.

HINWEIS: Nach dem Ende der Analyse müssen alle relevanten Daten auf eine sichere Art und Weise zerstört werden. Das beinhaltet auch das Zerstören des privaten Schlüssels, damit eine eventuell angefertigte unerlaubte Kopie der Secure-Trace-Dateien nicht mehr entschlüsselt werden kann.

H.323-Stack-Trace

Über diese Funktion ist die Einstellung H.323-Stack-Trace-Konfiguration durch einen Administrator mit dem Profil **Expert** möglich. Die Detailtiefe der Aufzeichnung kann über Trace-Levels (0 = geringste Detailtiefe bis 4 = größte Detailtiefe) definiert werden. Für die H.323-Stack-Trace-Ausgabe können folgende Einstellungen gewählt werden:

Trace-Ausgabe-Interface	Erläuterung	Standardeinstellung
Konsolen-Trace	**Konsolen-Trace aktivieren** H.323-Stack-Trace-Meldungen werden auf der Konsole ausgegeben.	Nicht aktiviert
Datei-Trace	**Datei-Trace aktivieren** H.323-Stack-Trace-Meldungen werden in eine Protokolldatei eingetragen. Bei aktivierter Option gelten folgende Einstellungen: Max. Größe des Trace-Buffers = 50000 Byte (Menge der Daten, die im Zwischenspeicher gehalten wird.) Max. Größe der Trace-Datei = 1000000 Byte (Maximale Größe der Protokolldatei.) Trace-Timer = 60 s (Verzögerungszeit, bis Daten in die Protokolldatei geschrieben werden.)	Nicht aktiviert

Durch das Aktivieren und/oder Deaktivieren von H.323-Modulen wird definiert, für welche Komponenten der H.323-Stack-Trace die Prozess- und Zustandsinformationen aufzeichnen soll. Der Status jedes H.323-Moduls wird durch die Farbe des zugehörigen Listenpunkts angezeigt (grün = H.323-Modul aktiviert, rot = H.323-Modul nicht aktiviert).

Das H.323-Stack-Trace-Protokoll kann auf einen PC übertragen oder gelöscht werden.

Lizenz-Komponenten-Trace

Diese Funktion dient zur Überwachung des systeminternen Lizenzagenten CLA (Customer License Agent) durch einen Administrator mit dem Profil Expert. Die Detailtiefe der Aufzeichnung kann über Trace-Levels (Niedrig = geringste Detailtiefe (Standardeinstellung), Standard = mittlere Detailtiefe, Alles = größte Detailtiefe) eingestellt werden.

In der Standardeinstellung ist der Lizenz-Komponenten-Trace aktiviert (Trace-Level = Niedrig).

Eine Änderung des Trace-Levels wirkt sich negativ auf die System-Performance aus und darf nur durch erfahrene Administratoren und nur in Absprache mit dem zuständigen Service-Support erfolgen.

Trace-Profile

Trace-Profile legen fest, welche Daten in welcher Detailtiefe aufgezeichnet werden sollen. Einem Trace-Profil werden Trace-Komponenten zugewiesen. Auf diese Weise wird festgelegt, für welche Systemkomponenten ein Trace-Profil die Prozess- und Zustandsinformationen aufzeichnen soll.

Es stehen vordefinierte Trace-Profile zur Verfügung, die alle Standardszenarios adressieren. Zusätzlich kann ein Administrator mit dem Profil **Expert** eigene Trace-Profile anlegen. Durch Starten eines Trace-Profils wird die Aufzeichnung über dieses Profil aktiviert und durch Stoppen deaktiviert.

- Ein Administrator mit dem Profil **Advanced** kann über den Wizard **Trace** Trace-Profile starten und/oder stoppen. Der Status jedes Trace-Profils wird durch die Farbe des zugehörigen Listenpunkts angezeigt (grün = Trace-Profil aktiviert, rot = Trace-Profil nicht aktiviert). Durch Auswahl von **Start/Stop** kann ein nicht aktives Trace-Profil (roter Listenpunkt) aktiviert/gestartet und ein aktives Trace-Profil (grüner Listenpunkt) deaktiviert/gestoppt werden
  Über **Trace laden** können die resultierenden Protokolldateien auf einen PC übertragen oder geöffnet werden.
  Über **Trace löschen** können die resultierenden Protokolldateien gelöscht werden.
  Beschrieben ist die Vorgehensweise für folgende Funktionen, die über den Wizard gestartet werden können:
  - *Wie Sie eine Systemtrace-Protokolldatei herunterladen*
  - *Wie Sie eine Systemtrace-Protokolldatei löschen*
  - *Wie Sie alle Trace-Profile anzeigen*
  - *Wie Sie ein Trace-Profil starten oder stoppen*
  - *Wie Sie Diagnosedaten / Diagnose-Protokolle herunterladen*
- Ein Administrator mit dem Profil **Expert** kann über den **Experten-Modus** alle Trace-Profile gemeinsam stoppen und Trace-Profile einzeln starten und/oder stoppen.
  Bei der Darstellung im Menübaum kennzeichnet die Farbe des Listenpunkts den Status des Trace-Profils (grün = Trace-Profil aktiviert, rot = Trace-Profil nicht aktiviert). Durch Auswahl von **Trace-Profil starten/stoppen** kann ein nicht aktives Trace-Profil (roter Listenpunkt) aktiviert/gestartet und ein aktives Trace-Profil (grüner Listenpunkt) deaktiviert/gestoppt werden.
  Durch Auswahl von **Trace-Profil anzeigen** werden die Detaildaten des gewünschten Trace-Profils angezeigt: Diese beinhalten neben dem Profilnamen, Angaben zum Schreibschutz und zum Status des Profils auch Informationen darüber, bei welchen Problemen dieses Trace-Profil verwendet werden sollte. Angegeben ist auch, welche Trace-Komponenten zum Trace-Profil gehören.

Trace-Profil	Anwendungsfall
Actors_Sensors_Door-Opener	Information liegt noch nicht vor!
Basic	Information liegt noch nicht vor!
Calls_with_Analog_Subscriber_Trunks	Information liegt noch nicht vor!
Calls_with_ISDN_Subscriber_Trunks	Information liegt noch nicht vor!
Calls_with_System_Device_HFA	Information liegt noch nicht vor!
Calls_with_System_Device_Upn	Information liegt noch nicht vor!
CDR_Charging_data	Information liegt noch nicht vor!
CMI	Information liegt noch nicht vor!
CSTA_application	Information liegt noch nicht vor!
Display_problems	Information liegt noch nicht vor!
Gateway_Stream_detailed	Information liegt noch nicht vor!
Gateway_Stream_overview	Information liegt noch nicht vor!
IP_Interfaces	Information liegt noch nicht vor!
License_problem	Information liegt noch nicht vor!
Network_Call_Routing_LCR	Information liegt noch nicht vor!
Peripheral_cards	Information liegt noch nicht vor!
RAS_or_Internal_access	Information liegt noch nicht vor!
Ressources_MOH_Conferencing	Information liegt noch nicht vor!
SIP_Interconnection_Subscriber_ITSP	Information liegt noch nicht vor!
SIP_Registration	Information liegt noch nicht vor!
Smart_VM	Information liegt noch nicht vor!
UC_Smart	Information liegt noch nicht vor!
Voice_Fax_connection	Information liegt noch nicht vor!
VPN	Information liegt noch nicht vor!
Web_based_Assistant_Expert_Mode	Information liegt noch nicht vor!
Xpression_Compact	Information liegt noch nicht vor!

Trace-Komponenten

Anhand von Trace-Komponenten werden die Prozess- und Zustandsinformationen einzelner Komponenten des Kommunikationssystems aufgezeichnet.

Alle Trace-Komponenten können durch einen Administrator mit dem Profil **Expert** gemeinsam gestoppt und einzeln gestartet oder gestoppt werden. Durch Starten einer Trace-Komponente wird die Aufzeichnung aktiviert und durch Stoppen deaktiviert. Die Detailtiefe der Aufzeichnung kann über Trace-Levels (0 = geringste Detailtiefe bis 9 = größte Detailtiefe) eingestellt werden.

Bei der Darstellung im Menübaum kennzeichnet die Farbe des Listenpunkts den Status der Trace-Komponente (grün = Trace-Komponente aktiviert, rot = Trace-

Komponente nicht aktiviert). Durch Auswahl von **Trace-Komponente starten/ stoppen** kann eine nicht aktive Trace-Komponente (roter Listenpunkt) aktiviert/ gestartet und eine aktive Trace-Komponente (grüner Listenpunkt) deaktiviert/ gestoppt werden.

Bei der Anzeige einer Trace-Komponente werden der Subsystem-Name, der Trace-Komponenten-Index, das eingestellte Trace-Level sowie die Statusinformation angezeigt, ob die Trace-Komponente aktuell gestartet ist oder nicht. Soll eine Trace-Komponente bearbeitet werden, kann neben der Änderung des Trace-Levels auch ein Start oder Stopp der Trace-Komponente vorgenommen werden.

24.8.4.1 Wie Sie eine Systemtrace-Protokolldatei herunterladen

Mit dem Wizard **Trace** können Sie Systemtrace-Protokolldateien herunterladen.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Diagnose > Trace**.

3) Klicken Sie auf **Diagnosedaten**.

4) Klicken Sie auf **Kein Protokoll**, um die Kontrollkästchen aller Protokolle zu deaktivieren.

5) Aktivieren Sie das Kontrollkästchen **Trace-Protokoll**.

6) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie das gesamte vorhandene Systemtrace-Protokoll herunterladen möchten, wählen Sie in der Aufklappliste **Gesamtes Protokoll** aus.
- Wenn Sie das Systemtrace-Protokoll des heutigen Tages herunterladen möchten, wählen Sie in der Aufklappliste **Protokoll von heute** aus.
- Wenn Sie das Systemtrace-Protokoll eines bestimmten Zeitraums herunterladen möchten, wählen Sie in der Aufklappliste **Eigene Auswahl** aus. Wählen Sie in der Aufklappliste **Von:** den Anfang und in der Aufklappliste **Bis:** das Ende des gewünschten Zeitraums aus.

7) Klicken Sie auf **Laden** und anschließend auf **OK**. Es erscheint das Dateidownload-Fenster.

8) Speichern Sie die Datei im gewünschten Verzeichnis. Schließen Sie anschließend das Fenster, das den Download der Datei bestätigt.

9) Klicken Sie auf **Weiter** und anschließend auf **Beenden**.

24.8.4.2 Wie Sie eine Systemtrace-Protokolldatei löschen

Mit dem Wizard **Trace** können Sie Systemtrace-Protokolldateien löschen.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Diagnose > Trace**.

3) Klicken Sie auf **Trace löschen** und anschließend auf **OK**.

4) Klicken Sie auf **Weiter** und anschließend auf **Beenden**.

24.8.4.3 Wie Sie alle Trace-Profile anzeigen

Mit dem Wizard **Trace** können Sie sich über den Status aller Trace-Profile informieren.

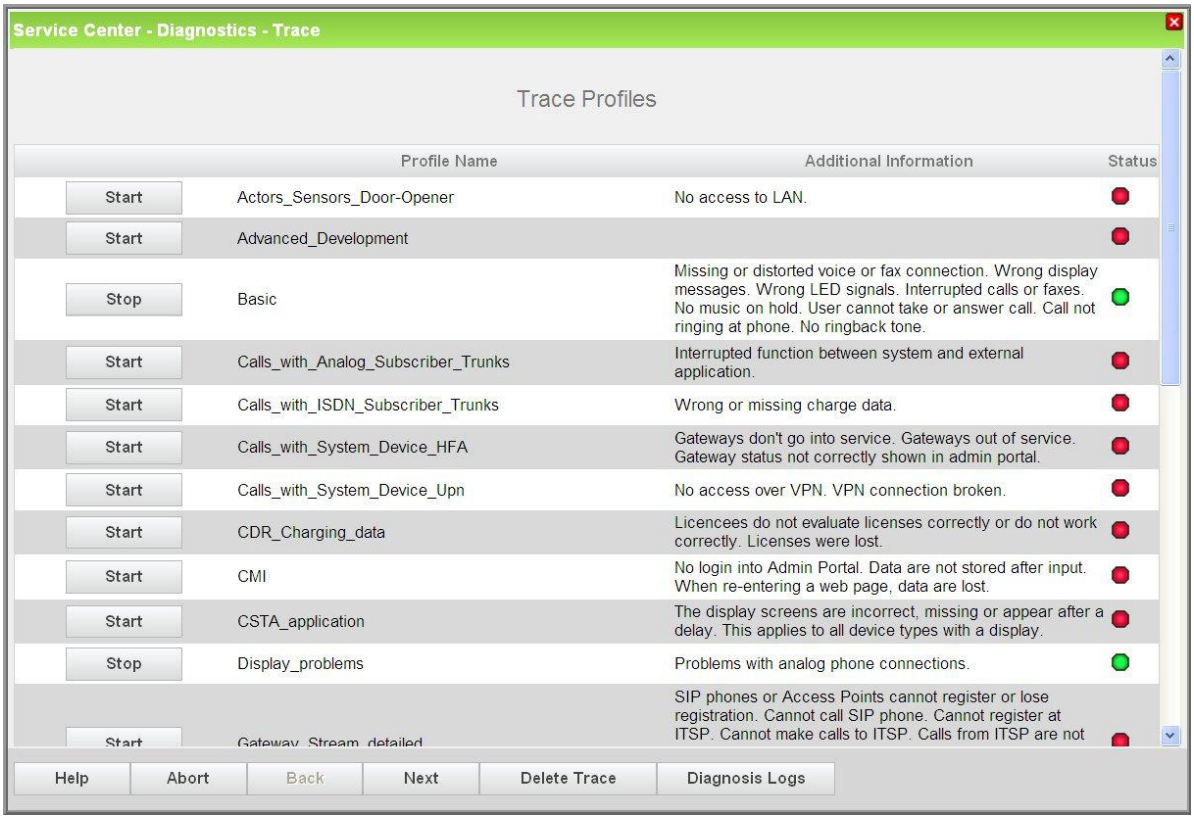
Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Diagnose > Trace**. Es wird Ihnen eine Liste aller Trace-Profile angezeigt und welche Trace-Profile gestartet sind und welche nicht gestartet sind.



3) Klicken Sie auf **Weiter** und anschließend auf **Beenden**.

24.8.4.4 Wie Sie ein Trace-Profil starten oder stoppen

Mit dem Wizard **Trace** können Sie Trace-Profile starten und stoppen.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Diagnose > Trace**. Es wird Ihnen eine Liste aller Trace-Profile angezeigt. Ein roter Listenpunkt kennzeichnet die Trace-Profile, die gestartet werden können. Ein grüner Listenpunkt kennzeichnet die Trace-Profile, die gestoppt werden können.

3) Wählen Sie eine der folgenden Möglichkeiten:

- Wie Sie ein Trace-Profil starten möchten, klicken Sie auf **Start**. Die Farbe des Listenpunkts, die den Status des zugehörigen Trace-Profils anzeigt, wechselt von rot nach grün.

HINWEIS: Gestartete Trace-Profile wirken sich negativ auf die System-Performance aus. Stoppen Sie deshalb alle Trace-Profile nach Beendigung Ihrer Diagnosetätigkeiten mit Ausnahme des Trace-Profils **Default**. Das Trace-Profil **Default** muss aktiv bleiben.

- Wie Sie ein Trace-Profil stoppen möchten, klicken Sie auf **Stop**. Die Farbe des Listenpunkts, die den Status des zugehörigen Trace-Profils anzeigt, wechselt von grün nach rot.

4) Klicken Sie auf **Weiter** und anschließend auf **Beenden**.

24.8.4.5 Wie Sie die Trace-Format-Konfiguration anzeigen oder ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.
- Eine Aufforderung des zuständigen Service-Supports zur Änderung der Trace-Format-Konfiguration liegt vor.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung > Traces**.

3) Klicken Sie im Menübaum auf **Traces > Trace-Format-Konfiguration**. Es werden Ihnen die aktuellen Einstellungen der Trace-Format-Konfiguration angezeigt.

4) Ändern Sie bei Bedarf die gewünschten Einstellungen.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.8.4.6 Wie Sie die Trace-Ausgabe-Interfaces anzeigen oder ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.
- Eine Aufforderung des zuständigen Service-Supports zur Änderung der Trace-Ausgabe-Interfaces liegt vor.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung > Traces**.

3) Klicken Sie im Menübaum auf **Traces > Trace-Ausgabe-Interfaces**. Es werden Ihnen die aktuellen Einstellungen der Trace-Ausgabe-Interfaces angezeigt.

4) Ändern Sie bei Bedarf die gewünschten Einstellungen.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.8.4.7 Wie Sie das Event Viewer-Protokoll / Kunden-Trace-Protokoll anzeigen oder ändern

Mit dem Wizard **Event Viewer** können Sie die Ereignis-Anzeige (Kunden-Trace) starten und die Aktualisierungs-Einstellung ändern.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Diagnose > Event Viewer**.

3) Klicken Sie auf die Registerkarte **Anzeigen**.

4) Wählen Sie die gewünschte Einstellung aus:

- Wenn das Protokoll automatisch aktualisiert werden soll, aktivieren Sie das Kontrollkästchen **Autom. Aktualisierung**.
- Wenn das Protokoll nicht automatisch aktualisiert werden soll, deaktivieren Sie das Kontrollkästchen **Autom. Aktualisierung**.

5) Klicken Sie bei Bedarf auf **Aktualisieren**, um das Kunden-Trace-Protokoll manuell zu aktualisieren.

6) Klicken Sie auf **Beenden**.

24.8.4.8 Wie Sie das Event Viewer-Protokoll / Kunden-Trace-Protokoll herunterladen oder öffnen

Mit dem Wizard **Event Viewer** können Sie die Kunden-Trace-Protokolldatei auf einen PC übertragen oder öffnen.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Diagnose > Event Viewer**.

3) Klicken Sie auf die Registerkarte **Laden über HTTP**.

4) Klicken Sie auf **Laden** und anschließend auf **OK**. Es erscheint das Dateidownload-Fenster.

5) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie die Protokolldatei herunterladen möchten, klicken Sie auf **Speichern unter**. Speichern Sie die Datei im gewünschten Verzeichnis und schließen Sie anschließend das Fenster, das den Download der Datei bestätigt.
- Wenn Sie die Protokolldatei öffnen möchten, klicken Sie auf **Öffnen**. Anschließend wird der Inhalt der komprimierten Protokolldatei angezeigt.

6) Klicken Sie auf **Beenden**.

24.8.4.9 Wie Sie das Event Viewer-Protokoll / Kunden-Trace-Protokoll löschen

Mit dem Wizard **Event Viewer** können Sie die Kunden-Trace-Protokolldatei löschen.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
2) Klicken Sie im Navigationsbaum auf **Diagnose > Event Viewer**.
3) Klicken Sie auf die Registerkarte **Event-Viewer-Protokoll löschen**.
4) Klicken Sie auf **Protokoll löschen** und anschließend auf **OK**.
5) Klicken Sie auf **Beenden**.

24.8.4.10 Wie Sie M5T-Trace-Komponenten anzeigen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung > Traces**.
3) Klicken Sie im Menübaum auf **Traces > M5T-Trace-Komponenten**. Es wird Ihnen eine Liste aller M5T-Trace-Komponenten mit den aktuellen Einstellungen angezeigt. Darüber hinaus werden Ihnen im Menübaum die Namen aller M5T-Trace-Komponenten angezeigt. Ein farbiger Listenpunkt kennzeichnet den Status jeder einzelnen M5T-Trace-Komponente.

24.8.4.11 Wie Sie eine M5T-Trace-Komponente starten oder stoppen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.
- Eine Aufforderung des zuständigen Service-Supports zum Starten oder Stoppen einer M5T-Trace-Komponente liegt vor.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung > Traces**.

3) Klicken Sie im Menübaum auf **Traces > M5T-Trace-Komponenten**. Im Menübaum werden Ihnen die Namen aller M5T-Trace-Komponenten angezeigt. Ein roter Listenpunkt kennzeichnet die M5T-Trace-Komponenten, die gestartet werden können. Ein grüner Listenpunkt kennzeichnet die M5T-Trace-Komponenten, die gestoppt werden können.

4) Klicken Sie im Menübaum auf die gewünschte M5T-Trace-Komponente.

5) Klicken Sie auf die Registerkarte **Trace-Komponente starten/stoppen**.

6) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie eine M5T-Trace-Komponente starten möchten, klicken Sie auf **Start** und anschließend auf **OK**.
- Wenn Sie eine M5T-Trace-Komponente stoppen möchten, klicken Sie auf **Stop** und anschließend auf **OK**.

24.8.4.12 Wie Sie M5T-Trace-Komponenten ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.
- Eine Aufforderung des zuständigen Service-Supports zur Änderung der M5T-Trace-Komponenten liegt vor.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung > Traces**.

3) Klicken Sie im Menübaum auf **Traces > M5T-Trace-Komponenten**. Es wird Ihnen eine Liste aller M5T-Trace-Komponenten mit den aktuellen Einstellungen angezeigt.

4) Ändern Sie die gewünschten Einstellungen.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.8.4.13 Wie Sie den Secure Trace starten oder stoppen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung > Traces**.

3) Klicken Sie im Menübaum auf **Traces > Secure Trace**.

4) Klicken Sie auf die Registerkarte **Secure Trace starten/beenden**.

5) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie den Secure Trace starten möchten, gehen Sie folgendermaßen vor:

  Geben Sie im Feld **Secure Trace Aktivierungs-Passphrase** das Passwort für den Secure Trace ein.

  Geben Sie im Feld **Dauer des Secure Trace (Min.)** die Zeit in Minuten ein, die der Secure Trace aktiv sein soll.

  Aktivieren Sie die Kontrollkästchen der Protokolle für die der Secure Trace erstellt werden soll. Deaktivieren Sie die Kontrollkästchen der Protokolle für die der Secure Trace nicht erstellt werden soll.

  Klicken Sie auf **Secure Trace einschalten** und anschließend auf **OK**.

- Wenn Sie den Secure Trace stoppen möchten, klicken Sie auf **Secure Trace beenden** und anschließend auf **OK**.

24.8.4.14 Wie Sie den Status des Secure Trace abfragen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung > Traces**.

3) Klicken Sie im Menübaum auf **Traces > Secure Trace**.

4) Klicken Sie auf die Registerkarte **Secure Trace Status**. Anschließend wird der aktuelle Status des Secure Trace angezeigt.

24.8.4.15 Wie Sie das Passwort für den Secure Trace ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung > Traces**.
3) Klicken Sie im Menübaum auf **Traces > Secure Trace**.
4) Klicken Sie auf die Registerkarte **Secure Trace Passphrase ändern**.
5) Geben Sie im Feld **Aktuelle Passphrase** das derzeitige Passwort für den Secure Trace ein.
6) Geben Sie in die Felder **Neue Passphrase** und **Neue Passphrase wiederholen** das neue, mindestens fünf- und maximal zwölfstellige Passwort für den Secure Trace ein.
7) Klicken Sie auf **Übernehmen**.

24.8.4.16 Wie Sie das Zertifikat für den Secure Trace aus einer X.509-Datei importieren

Voraussetzungen

- Eine X.509-Datei im PEM- oder Binärformat liegt vor.
- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung > Traces**.
3) Klicken Sie im Menübaum auf **Traces > Secure Trace**.
4) Klicken Sie auf die Registerkarte **X.509 Datei für Secure Trace importieren**.
5) Klicken Sie auf **Durchsuchen**, um die gewünschte X.509-Datei auszuwählen.
6) Klicken Sie auf **Öffnen**.
7) Klicken Sie auf **Zertifikat aus Datei importieren**.

24.8.4.17 Wie Sie die H.323-Stack-Trace-Konfiguration anzeigen oder ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.
- Eine Aufforderung des zuständigen Service-Supports zur Änderung der H.323-Stack-Trace-Konfiguration liegt vor.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung > Traces**.

3) Klicken Sie im Menübaum auf **Traces > H.323-Stack-Trace**.

4) Klicken Sie auf die Registerkarte **H.323-Stack-Trace-Konfiguration ändern**. Es werden Ihnen die aktuellen Einstellungen der H.323-Stack-Trace-Konfiguration angezeigt.

5) Ändern Sie bei Bedarf die gewünschten Einstellungen.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.8.4.18 Wie Sie H.323-Module ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.
- Eine Aufforderung des zuständigen Service-Supports zur Änderung der H.323-Module liegt vor.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung > Traces**.

3) Klicken Sie im Menübaum auf **Traces > H.323-Stack-Trace**.

4) Klicken Sie auf die Registerkarte **Alle H.323-Module ändern**.

5) Wählen Sie die gewünschte Einstellung für **Trace an** aus:

- Wenn Sie den Trace für bestimmte H.323-Module aktivieren möchten, aktivieren Sie die Kontrollkästchen der gewünschten H.323-Module. Deaktivieren Sie die Kontrollkästchen der H.323-Module, für die der Trace deaktiviert werden soll.
- Wenn Sie den Trace für alle H.323-Module deaktivieren möchten, klicken Sie auf **Keine**.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.8.4.19 Wie Sie das H.323-Stack-Trace-Protokoll herunterladen oder öffnen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung > Traces**.
3) Klicken Sie im Menübaum auf **Traces > H.323-Stack-Trace**.
4) Klicken Sie auf die Registerkarte **H.323-Stack-Trace-Protokoll über HTTP laden**.
5) Klicken Sie auf **Laden** und anschließend auf **OK**. Es erscheint das Dateidownload-Fenster.
6) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie die H.323-Stack-Trace-Protokolldatei speichern möchten, klicken Sie auf **Speichern unter**. Speichern Sie die Datei im gewünschten Verzeichnis und schließen Sie anschließend das Fenster, das den Download der Datei bestätigt.
   - Wenn Sie die H.323-Stack-Trace-Protokolldatei öffnen möchten, klicken Sie auf **Öffnen**. Die Datei wird anschließend im Texteditor angezeigt.

24.8.4.20 Wie Sie das H.323-Stack-Trace-Protokoll löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung > Traces**.
3) Klicken Sie im Menübaum auf **Traces > H.323-Stack-Trace**.
4) Klicken Sie auf die Registerkarte **H.323-Stack-Trace-Protokoll löschen**.
5) Klicken Sie auf **Protokoll löschen** und anschließend auf **OK**.

24.8.4.21 Wie Sie den Lizenz-Komponenten-Trace ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.
- Eine Aufforderung des zuständigen Service-Supports zur Änderung des Lizenz-Komponenten-Trace liegt vor.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung > Traces**.

3) Klicken Sie im Menübaum auf **Traces > Lizenz-Komponente > CLA**.

4) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie den Lizenz-Komponenten-Trace stoppen möchten, wählen Sie in der Aufklappliste **Trace-Level** den Eintrag **Aus** aus.
- Wenn Sie eine niedrige Detailtiefe für die Trace-Aufzeichnung möchten, wählen Sie in der Aufklappliste **Trace-Level** den Eintrag **Niedrig** aus.
- Wenn Sie eine mittlere Detailtiefe für die Trace-Aufzeichnung möchten, wählen Sie in der Aufklappliste **Trace-Level** den Eintrag **Standard** aus.
- Wenn Sie eine große Detailtiefe für die Trace-Aufzeichnung möchten, wählen Sie in der Aufklappliste **Trace-Level** den Eintrag **Alles** aus.

5) Klicken Sie auf **Übernehmen**.

24.8.4.22 Wie Sie Details eines Trace-Profils anzeigen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung > Traces**.

3) Klicken Sie im Menübaum auf **Traces > Trace-Profile**. Es wird Ihnen eine Liste aller Trace-Profile angezeigt. Darüber hinaus werden Ihnen im Menübaum die Namen aller Trace-Profile angezeigt. Ein farbiger Listenpunkt kennzeichnet den Status jedes einzelnen Trace-Profils.

4) Klicken Sie im Menübaum auf den Namen des gewünschten Trace-Profils. Es werden Ihnen die Detaildaten dieses Trace-Profils angezeigt.

24.8.4.23 Wie Sie alle Trace-Profile stoppen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung > Traces**.
3) Klicken Sie im Menübaum auf **Traces > Trace-Profile**.
4) Klicken Sie auf die Registerkarte **Alle Trace-Profile stoppen**.
5) Klicken Sie auf **Alle stoppen** und anschließend auf **OK**.

24.8.4.24 Wie Sie ein Trace-Profil hinzufügen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung > Traces**.
3) Klicken Sie im Menübaum auf **Traces > Trace-Profile**.
4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Sie ein leeres Trace-Profil hinzuzufügen möchten, klicken Sie auf die Registerkarte **Trace-Profil hinzufügen (leeres Profil)**.
   - Wenn Sie ein Trace-Profil hinzuzufügen möchten, das die Trace-Komponenten aller aktuell gestarteten Trace-Profile enthält, klicken Sie auf die Registerkarte **Trace-Profil hinzufügen (mit aktuellen Trace-Einstellungen)**. Wählen Sie aus, welche der angezeigten Trace-Komponenten mit welchem Level in dem neuen Trace-Profil enthalten sein sollen.
5) Geben Sie im Feld **Profilname** den Namen des neuen Trace-Profils ein.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.8.4.25 Wie Sie Trace-Komponenten anzeigen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung > Traces**.
3) Klicken Sie im Menübaum auf **Traces > Trace-Komponenten**.
4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn die Liste aller Trace-Komponenten angezeigt werden soll, klicken Sie auf die Registerkarte **Alle Trace-Komponenten anzeigen**.
   - Wenn die Liste aller gestarteten Trace-Komponenten angezeigt werden soll, klicken Sie auf die Registerkarte **Gestartete Trace-Komponenten anzeigen**.
   - Wenn die Liste aller gestoppten Trace-Komponenten angezeigt werden soll, klicken Sie auf die Registerkarte **Gestoppte Trace-Komponenten anzeigen**.

24.8.4.26 Wie Sie Details einer Trace-Komponente anzeigen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung > Traces**.
3) Klicken Sie im Menübaum auf **Traces > Trace-Komponenten**. Es wird Ihnen eine Liste aller Trace-Komponenten angezeigt. Darüber hinaus werden Ihnen im Menübaum die Namen aller Trace-Komponenten angezeigt. Ein farbiger Listenpunkt kennzeichnet den Status jeder einzelnen Trace-Komponente.
4) Klicken Sie im Menübaum auf den Namen der gewünschten Trace-Komponente. Es werden Ihnen die Detaildaten dieser Trace-Komponente angezeigt.

24.8.4.27 Wie Sie eine Trace-Komponente starten oder stoppen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung > Traces**.
3) Klicken Sie im Menübaum auf **Traces > Trace-Komponenten**. Im Menübaum werden Ihnen die Namen aller Trace-Komponenten angezeigt. Ein roter Listenpunkt kennzeichnet die Trace-Komponenten, die gestartet

werden können. Ein grüner Listenpunkt kennzeichnet die Trace-Komponenten, die gestoppt werden können.

4) Klicken Sie im Menübaum auf die gewünschte Trace-Komponente.

5) Klicken Sie auf die Registerkarte **Trace-Komponente starten/stoppen**.

6) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie eine Trace-Komponente starten möchten, klicken Sie auf **Start** und anschließend auf **OK**.
- Wenn Sie eine Trace-Komponente stoppen möchten, klicken Sie auf **Stop** und anschließend auf **OK**.

24.8.4.28 Wie Sie alle Trace-Komponenten stoppen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung > Traces**.

3) Klicken Sie im Menübaum auf **Traces > Trace-Komponenten**.

4) Klicken Sie auf die Registerkarte **Alle Trace-Komponenten stoppen**.

5) Klicken Sie auf **Alle stoppen** und anschließend auf **OK**.

24.8.4.29 Wie Sie Trace-Komponenten ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung > Traces**.

3) Klicken Sie im Menübaum auf **Traces > Trace-Komponenten**.

4) Klicken Sie auf die Registerkarte **Trace-Komponenten ändern**. Es wird Ihnen eine Liste aller Trace-Komponenten mit den aktuellen Einstellungen angezeigt.

5) Ändern Sie die gewünschten Einstellungen.

6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.8.5 TCP-Dump

Ein TCP-Dump dient zur Überwachung und Auswertung des Datenverkehrs in einer IP-Vernetzung.

> ***INFO:*** Das Aktivieren eines TCP-Dumps wirkt sich negativ auf die System-Performance aus und darf nur durch erfahrene Administratoren und nur in Absprache mit dem zuständigen Service-Support erfolgen.

TCP-Dump-Dateien werden im Kommunikationssystem gespeichert. Für die Diagnose der Dateien ist eine entsprechende Applikation erforderlich.

TCP-Dumps werden häufig eingesetzt, um

- für einen kurzen Zeitraum (zum Beispiel für ein reproduzierbares Fehlerbild) einen LAN-Trace zu erzeugen.
- autorisierten Servicetechnikern den Fernzugriff auf einen LAN-Trace zu ermöglichen, beispielsweise über SSDP.

Vorteile gegenüber RPCAP-Dämon: Fernzugriff möglich, Trace-Dateien müssen nicht per E-Mail verschickt werden

Nachteile gegenüber RPCAP-Dämon: Langzeit-Traces nicht sinnvoll, begrenzter Speicherplatz, keine Capture-Filter einstellbar, aufwendigere Handhabung bei vielen Einzel-Traces

24.8.5.1 Wie Sie einen TCP-Dump starten

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Traces > TCP-Dump**.

3) Klicken Sie auf **TCP-Dump starten**.

4) Wählen Sie die gewünschten Einstellungen.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.8.5.2 Wie Sie einen TCP-Dump stoppen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Traces > TCP-Dump**.

3) Klicken Sie auf **TCP-Dump beenden**.

4) Klicken Sie auf **OK**.

24.8.5.3 Wie Sie einen TCP-Dump löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Traces > TCP-Dump**.

3) Klicken Sie auf **TCP-Dump aufräumen**.

4) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.8.6 RPCAP-Dämon

Ein RPCAP (Remote Packet Capture)-Dämon dient zur Überwachung und Auswertung des Datenverkehrs in einer IP-Vernetzung.

INFO: Das Aktivieren eines RPCAP-Dämons wirkt sich negativ auf die System-Performance aus und darf nur durch erfahrene Administratoren und nur in Absprache mit dem zuständigen Service-Support erfolgen.

Über den RPCAP-Dämon wird ein Fernzugriff externer Applikationen auf die TCP/IP-Pakete der LAN-Schnittstellen des Kommunikationssystems ermöglicht.

Ein RPCAP-Dämon wird häufig für Langzeit-Traces eingesetzt, da die Trace-Dateien auf einem PC und nicht im Kommunikationssystem abgelegt werden.

Vorteile gegenüber TCP-Dump: Schnellere und einfachere Handhabung, Langzeit-Traces möglich, Anzahl und/oder Größe der Trace-Dateien frei wählbar, Trace des internen LAN möglich

Nachteile gegenüber TCP-Dump: Doppelter Datenverkehr im Netz und dadurch höhere Belastung der LAN-Schnittstellen des Kommunikationssystems, spezielle Portfreigabe nötig (Firewall)

24.8.6.1 Wie Sie den RPCAP-Dämon aktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.
- Der RPCAP-Dämon wurde deaktiviert.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Traces > RPCAP Dämon**.

3) Wählen Sie die gewünschten Einstellungen.

4) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.8.6.2 Wie Sie den RPCAP-Dämon deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.
- Der RPCAP-Dämon wurde aktiviert.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

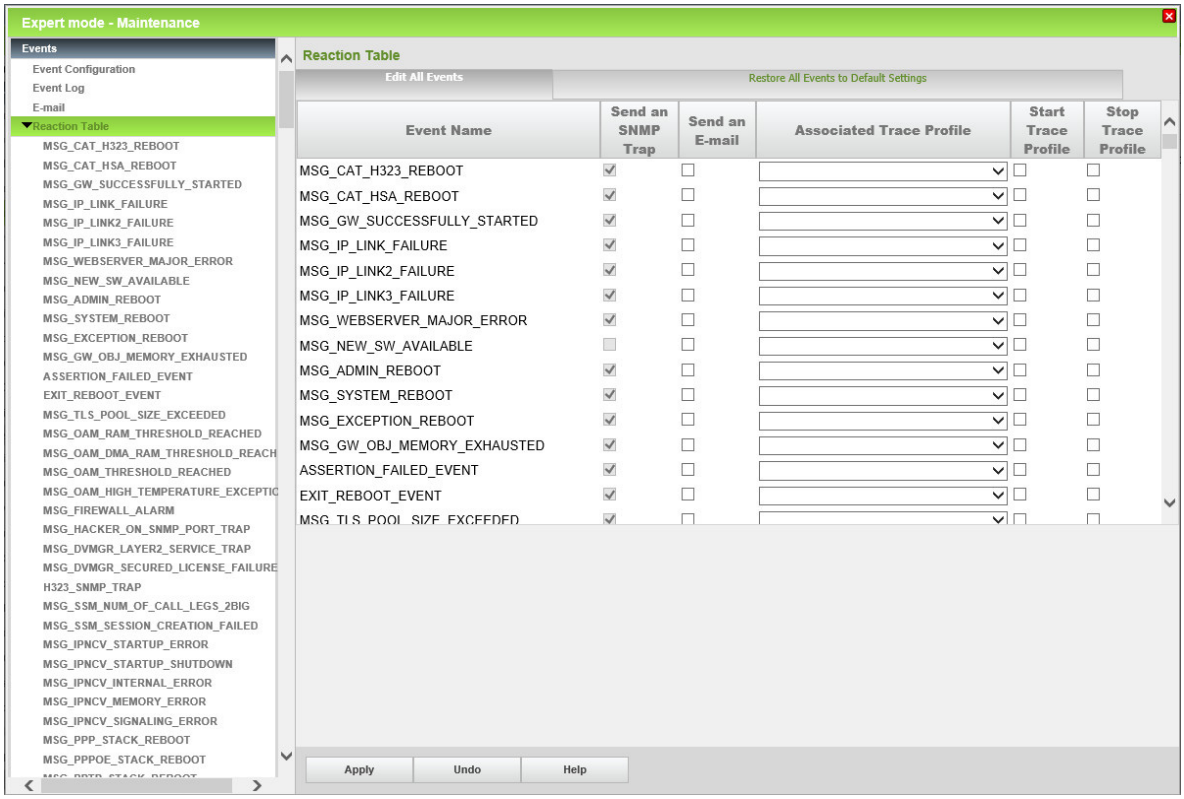
2) Klicken Sie im Navigationsbaum auf **Traces > RPCAP Dämon**.

3) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.8.7 Events

Events (Ereignisse) informieren über Mängel des Kommunikationssystems. Alle Events werden in eine Protokolldatei beschränkter Größe geschrieben. Ist die maximale Größe der Datei überschritten, wird eine neue Datei angelegt. Es können bis zu sieben Dateien entstehen.

Abhängig von der Einstellung in der Reaktionstabelle und der Problemklasse können Events einen SNMP-Trap erzeugen, eine E-Mail auslösen und/oder eine Trace-Überwachung starten/stoppen. Die Auswertung, Konfiguration und Speicherung des Event Logs (der Ereignisanzeige) ist über das WBM möglich.



Um die Event-Protokolldatei zu interpretieren, muss die Datei mit dem WBM heruntergeladen und extrahiert werden. Anschließend kann die Datei mit einem beliebigen Texteditor geöffnet und bearbeitet oder ausgedruckt werden. Nachdem die Event-Protokolldatei übertragen wurde, kann die Datei aus dem Speicher des Kommunikationssystems gelöscht werden.

Events, die Aktionen auslösen können, sind durch folgende Eigenschaften definiert:

- Event-Code:
  Kennzeichnet ein Event (Ereignis), wie zum Beispiel `MSG_ADMIN_LOGGED_OUT` = Information über das Logout eines Administrators.
- Event-Typ:
  Es gibt folgende verschiedene Typen:
  - Information: Reine Statusmeldung, keine Fehlermeldung.
  - Warning: Meldung über einen möglicherweise problematischen Vorgang oder Zustand, jedoch keine Fehlermeldung.
  - Minor: Fehlermeldung. Der Fehler hat keine problematischen Auswirkungen.
  - Major: Fehlermeldung. Der Fehler kann problematische Auswirkungen haben.
  - Critical: Fehlermeldung. Der Fehler hat problematische Auswirkungen.
  - Cleared: Fehlermeldung. Der Fehler wurde vom Kommunikationssystem bereits behoben.

  - Indeterminate: Fehlermeldung. Die Fehlerursache ist nicht genau bestimmbar.
- Event-Text
  Einige Event-Texte enthalten variable Daten. Diese sind folgendermaßen gekennzeichnet:
  - %s: Zeichenkette
  - %u: Positive oder negative Dezimalzahl
  - %f: Fließkommazahl
  - %p: Zeiger (Speicheradresse)
  - %x: Hexadezimalzahl (mit Kleinbuchstaben)
  - %X: Hexadezimalzahl (mit Großbuchstaben)
  - %c: Einzelnes Zeichen
  - %d und %i: Positive Dezimalzahl

Reaktionstabelle

Anhand der Reaktionstabelle kann ein Administrator mit dem Profil **Expert** für jeden möglichen Event getrennt definieren, wie bei dessen Eintreten reagiert werden soll.

Eingestellt werden kann, ob ein SNMP-Trap versendet werden soll, ob das Kommunikationssystem neu gestartet werden soll, ob eine E-Mail versendet werden soll und ob ein Trace-Profil gestartet oder gestoppt werden soll. Ist dem Event ein Trace-Profil zugeordnet, wird dessen Name angezeigt.

E-Mail-Einstellungen

Anhand dieser Einstellungen kann ein Administrator mit dem Profil **Expert** Angaben für den E-Mailversand bei Eintreten eines Events vornehmen.

Diagnose Logs

Das Kommunikationssystem protokolliert bestimmte Aktionen von Prozessen in Diagnose Logs. Diese Protokolldateien können für Diagnosezwecke durch einen Administrator mit dem Profil **Expert** ausgewertet werden.

Alarm-Signalisierung bei Temperaturüberschreitung

Im Kommunikationssystem sind zwei kritische Temperaturwerte gespeichert. Überschreitet die Temperatur des Systems den ersten Wert, erfolgt eine Warnmeldung per SNMP-Trap oder E-Mail, dass die Temperatur des Systems zu hoch ist. Zusätzlich kann diese Meldung auch im Display von bis zu 3 Systemtelefone (UP0 & HFA) angezeigt werden. Wird der zweite Wert überschritten, werden die für die Überhitzung verantwortlichen Baugruppen kontrolliert heruntergefahren (z. B. OpenScape Business Booster Card) oder abgeschaltet (z. B. SLAV/SLAD). Um den Alarm zu löschen und die Baugruppen wieder in Betrieb zu nehmen, muss das System ausgeschaltet und wieder neu eingeschaltet werden.

Es kann eingestellt werden, welche 3 Ziele (Systemtelefone) bei einer Temperaturüberschreitung benachrichtigt werden sollen.

24.8.7.1 Wie Sie die Event-Protokollierung über LAN ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung > Events**.

3) Klicken Sie im Menübaum auf **Events > Event-Konfiguration**.

4) Wählen Sie die gewünschte Einstellung aus:

- Wenn die Event-Protokollierung über ein LAN übertragen werden soll, aktivieren Sie das Kontrollkästchen **Event-Protokollierung über LAN aktivieren**.
- Wenn keine Event-Protokollierung über ein LAN übertragen werden soll, deaktivieren Sie das Kontrollkästchen **Event-Protokollierung über LAN aktivieren**.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.8.7.2 Wie Sie eine Event-Protokolldatei herunterladen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung > Events**.

3) Klicken Sie im Menübaum auf **Events > Event-Protokoll**.

4) Klicken Sie auf die Registerkarte **Laden über HTTP**.

5) Klicken Sie auf **Laden** und anschließend auf **OK**. Es erscheint das Datei-download-Fenster.

6) Speichern Sie die Datei im gewünschten Verzeichnis. Schließen Sie anschließend das Fenster, das den Download der Datei bestätigt.

24.8.7.3 Wie Sie eine Event-Protokolldatei löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung > Events**.
3) Klicken Sie im Menübaum auf **Events > Event-Protokoll**.
4) Klicken Sie auf die Registerkarte **Event-Protokoll löschen**.
5) Klicken Sie auf **Protokoll löschen** und anschließend auf **OK**.

24.8.7.4 Wie Sie E-Mail-Einstellungen für Events ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung > Events**.
3) Klicken Sie im Menübaum auf **Events > E-Mail**.
4) Geben Sie als **Betreff** ein, was in den E-Mails im Betreff-Feld angezeigt werden soll.

   INFO: Der Betreff sollte eindeutig darauf hinweisen, dass es sich um eine E-Mail aufgrund eines Events handelt.

5) Geben Sie in den Feldern **Empfänger 1** bis **Empfänger 5** die E-Mail-Adressen ein, an die die E-Mails verschickt werden sollen.
6) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.8.7.5 Wie Sie die Event-Reaktionstabelle anzeigen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Wartung > Events**.
3) Klicken Sie im Menübaum auf **Events > Reaktionstabelle**. Es wird Ihnen die Reaktionstabelle mit allen möglichen Events und deren Einstellungen angezeigt.

24.8.7.6 Wie Sie Reaktionseinstellungen eines Events ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung > Events**.

3) Klicken Sie im Menübaum auf **Events > Reaktionstabelle**. Es wird Ihnen die Reaktionstabelle mit allen möglichen Events und deren Einstellungen angezeigt. Darüber hinaus werden Ihnen im Menübaum die Namen aller möglichen Events angezeigt.

4) Klicken Sie im Menübaum auf den Namen des gewünschten Events.

5) Klicken Sie auf die Registerkarte **Event bearbeiten**. Es werden Ihnen die Reaktionseinstellungen des gewünschten Events angezeigt.

> ***INFO:*** Die Reaktionseinstellungen **Gateway neu starten** und **OpenScape benachrichtigen** können Sie nicht ändern. Eine Änderung der Einstellung **SNMP-Trap senden** ist nicht bei allen Events möglich.

6) Falls möglich, wählen Sie die Einstellung für **SNMP-Trap senden**:

- Wenn bei Eintreten des Events ein SNMP-Trap gesendet werden soll, aktivieren Sie das Kontrollkästchen **SNMP-Trap senden**.
- Wenn bei Eintreten des Events kein SNMP-Trap gesendet werden soll, deaktivieren Sie das Kontrollkästchen **SNMP-Trap senden**.

7) Wählen Sie die Einstellung für **E-Mail versenden**:

- Wenn bei Eintreten des Events eine E-Mail gesendet werden soll, aktivieren Sie das Kontrollkästchen **E-Mail versenden**.
- Wenn bei Eintreten des Events keine E-Mail gesendet werden soll, deaktivieren Sie das Kontrollkästchen **E-Mail versenden**.

8) Wählen Sie in der Aufklappliste **Zugeordnetes Trace-Profil** das gewünschte Trace-Profil aus.

9) Wählen Sie die Einstellung für den Start oder Stopp des Trace-Profils:

- Wenn bei Eintreten des Events das ausgewählte Trace-Profil gestartet werden soll, aktivieren Sie das Kontrollkästchen **Trace-Profil starten**.
- Wenn bei Eintreten des Events das ausgewählte Trace-Profil gestoppt werden soll, aktivieren Sie das Kontrollkästchen **Trace-Profil stoppen**.

10) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.8.7.7 Wie Sie Reaktionseinstellungen mehrerer Events ändern

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung > Events**.

3) Klicken Sie im Menübaum auf **Events > Reaktionstabelle**. Es wird Ihnen die Reaktionstabelle mit allen möglichen Events und deren Reaktionseinstellungen angezeigt.

> ***INFO:*** Die Reaktionseinstellungen **Gateway neu starten** und **OpenScape benachrichtigen** können Sie nicht ändern. Eine Änderung der Einstellung **SNMP-Trap senden** ist nicht bei allen Events möglich.

4) Ändern Sie die Reaktionseinstellungen der gewünschten Events in der Reaktionstabelle:

- Falls möglich, wählen Sie die Einstellung für **SNMP-Trap senden**:

  Wenn bei Eintreten des Events ein SNMP-Trap gesendet werden soll, aktivieren Sie das Kontrollkästchen **SNMP-Trap senden**.

  Wenn bei Eintreten des Events kein SNMP-Trap gesendet werden soll, deaktivieren Sie das Kontrollkästchen **SNMP-Trap senden**.

- Wählen Sie die Einstellung für **E-Mail versenden**:

  Wenn bei Eintreten des Events eine E-Mail gesendet werden soll, aktivieren Sie das Kontrollkästchen **E-Mail versenden**.

  Wenn bei Eintreten des Events keine E-Mail gesendet werden soll, deaktivieren Sie das Kontrollkästchen **E-Mail versenden**.

- Wählen Sie in der Aufklappliste **Zugeordnetes Trace-Profil** das gewünschte Trace-Profil aus.

- Wählen Sie die Einstellung für den Start oder Stopp des Trace-Profils:

  Wenn bei Eintreten des Events das ausgewählte Trace-Profil gestartet werden soll, aktivieren Sie das Kontrollkästchen **Trace-Profil starten**.

  Wenn bei Eintreten des Events das ausgewählte Trace-Profil gestoppt werden soll, aktivieren Sie das Kontrollkästchen **Trace-Profil stoppen**.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.8.7.8 Wie Sie Diagnose Logs herunterladen oder öffnen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung > Events**.

3) Klicken Sie im Menübaum auf **Events > Diagnose Logs**.

4) Klicken Sie auf die Registerkarte **Diagnose Logs holen**. Es wird Ihnen eine Liste aller verfügbaren Logs mit dem jeweiligen Dateinamen, der Dateigröße in Bytes, dem Zeitpunkt der letzten Änderung und den Dateiattributen angezeigt.

5) Klicken Sie unter **Dateiname** auf den Namen des gewünschten Diagnose Logs. Es erscheint das Dateidownload-Fenster.

6) Speichern Sie die Datei im gewünschten Verzeichnis. Schließen Sie anschließend das Fenster, das den Download der Datei bestätigt.

24.8.7.9 Wie Sie Diagnose Logs löschen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung > Events**.

3) Klicken Sie im Menübaum auf **Events > Diagnose Logs**. Es wird Ihnen eine Liste aller verfügbaren Logs mit dem jeweiligen Dateinamen, der Dateigröße in Bytes, dem Zeitpunkt der letzten Änderung und den Dateiattributen angezeigt.

4) Klicken Sie auf die Registerkarte **Diagnose Logs löschen**.

5) Klicken Sie auf **Protokoll löschen** und anschließend auf **OK**.

24.8.7.10 Wie Sie die Ziele für die Alarm-Signalisierung festlegen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung > Events**.

3) Klicken Sie im Menübaum auf **Events > Alarm-Signalisierung**.

4) Wählen Sie in den Aufklapplisten **Teilnehmer 1-3** die drei Ziele (Systemtelefone mit Display, UP0 & HFA) aus, die im Display benachrichtigt werden sollen, wenn die Temperatur des Systems einen fest eingestellten kritischen Wert übersteigt.

5) Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

24.8.8 Konfigurationsdaten für die Diagnose

Für Diagnosezwecke können "kleinere" Backup-Sets erzeugt werden, die Daten für die Fehlersuche durch den Service-Support enthalten. Im Gegensatz zu den normalen Backup-Sets werden wesentlich kleinere Datenmengen erzeugt und damit zum Beispiel ein einfaches Versenden per E-Mail ermöglicht.

Diagnose-Backup-Sets enthalten unter anderem die Konfigurationsdaten des Kommunikationssystems und der UC Applikation (UC Smart oder UC Suite). Sprachnachrichten, Faxnachrichten und Ansagen sind nicht enthalten.

Für die Sicherung von Diagnose-Backup-Sets können folgende Medien verwendet werden:

- **USB-Device**
  Die Daten können zum Beispiel auf eine angeschlossene USB-Festplatte oder einen angeschlossenen USB-Stick gesichert werden.

  HINWEIS: Soll eine USB-Festplatte, die Partition einer USB-Festplatte oder ein USB-Stick für die Sicherung verwendet werden, muss diese(r) mit FAT-32 formatiert sein. Vom einem NTFS formatierten USB-Medium kann nur gelesen werden. Sind mehrere Partitionen vorhanden, ist eine Sicherung nur auf der ersten Partition möglich.

  Wird auf ein bootfähiges USB-Medium gespeichert, ist dieses USB-Medium nach der Sicherung zu entfernen.

- **HTTPS**
  Die Daten können über HTTPS auf der Festplatte des Client-PC gesichert werden.
- **Hard Disk** (nur für OpenScape Business X3/X5/X8 mit UC Booster Card (Application Board OCAB))
  Die Daten können auf der Festplatte des Application Boards OCAB gesichert werden.

INFO: Eine Sicherung auf der Festplatte des Kommunikationssystems ist nicht möglich.

24.8.8.1 Wie Sie Konfigurationsdaten für die Diagnose erzeugen

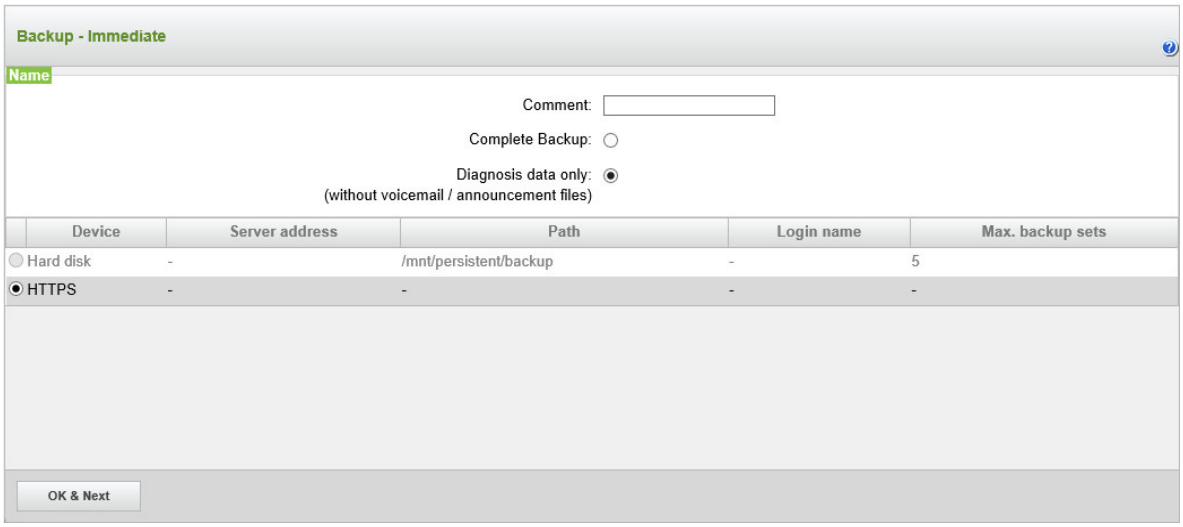
Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Datensicherung**.

2) Klicken Sie im Navigationsbaum auf **Datensicherung > Backup-sofort**.



3) Aktivieren Sie das Kontrollkästchen **Diagnose**.

4) Wählen Sie das Gerät aus, auf dem das Diagnose-Backup-Set gesichert werden soll. Sie haben folgende Möglichkeiten:

- Wenn Sie die Daten auf einer angeschlossenen USB-Festplatte oder einem angeschlossenen USB-Stick sichern möchten, aktivieren Sie das Optionsfeld **USB-Device**.
- Wenn Sie die Daten über HTTPS auf der Festplatte des Client-PC sichern möchten, aktivieren Sie das Optionsfeld **HTTPS**.
- Nur für OpenScape Business X3/X5/X8 mit UC Booster Card (Application Board OCAB): Wenn Sie die Daten auf der Festplatte des Application Boards OCAB sichern möchten, aktivieren Sie das Optionsfeld **Hard Disk**.

5) Geben Sie bei Bedarf im Feld **Kommentar** einen Kommentar zu Ihrem Diagnose-Backup-Set ein. Vermeiden Sie bei der Eingabe Umlaute und Sonderzeichen.

6) Klicken Sie auf **OK & Weiter**. In einem weiteren Fenster wird Ihnen der Fortschritt der Sicherung angezeigt.

7) Die Sicherung war erfolgreich, wenn die Meldung `Sicherung erfolgreich ausgeführt!` erscheint.

8) Wenn Sie als Backup-Medium **HTTPS** ausgewählt haben, müssen Sie das Diagnose-Backup-Set und die dazugehörige Text-Datei an einem Speicherort Ihrer Wahl sichern. Bei den anderen Backup-Medien geschieht dies automatisch. Das Browser-Fenster muss solange geöffnet bleiben, bis der Speichervorgang für Diagnose-Backup-Set und Text-Datei abgeschlossen ist.

> ***HINWEIS:*** Wenn Sie als Backup-Medium **USB-Device** ausgewählt haben, warten Sie ab, bis die LED des USB-Mediums aufhört zu blinken. Erst dann ist das Diagnose-Backup-Set vollständig auf dem USB-Medium gespeichert. Entfernen Sie anschließend das USB-Medium.

9) Klicken Sie auf **Beenden**.

Nächste Schritte

Das Diagnose-Backup-Set kann jetzt beispielsweise für die Fehlersuche an den zuständigen Service-Support per E-Mail verschickt werden.

24.8.9 Card Manager

Der Card Manager ist ein Tool, mit dem die Software des Kommunikationssystems auf eine SDHC-Karte geschrieben werden kann. Dazu wird die Software des Kommunikationssystems als Image-Datei benötigt.

Die Software auf der SDHC-Karte ist eine Standard-System-Software ohne Kundendaten. SDHC-Karten können nicht für Software-Updates oder das Sichern von Kundendaten verwendet werden.

Der Card Manager kann entweder als Java-Anwendung auf einem Linux-PC (auch in einer virtuellen Umgebung möglich) oder über eine Linux-Boot-DVD gestartet werden.

Anwendungsfälle

- Vor Auslieferung des Systems soll die Software durch die aktuellste Software getauscht werden.
- Die genutzte SDHC-Karte ist defekt und muss durch eine neue SDHC-Karte ausgetauscht werden, auf der noch keine Software gespeichert ist.
- Die genutzte Software ist defekt und muss neu aufgespielt werden. Dabei werden alle Kundendaten gelöscht.
  Ist zur Wiederherstellung der Kundendaten ein Backup-Set vorhanden, sollte die neu installierte Software mit der Software-Version übereinstimmen, mit der das Backup-Set erzeugt wurde, damit die im Backup-Set enthaltenen

Einstellungen auch von der installierten Software unterstützt und verarbeitet werden können.

Hard- und Softwarevoraussetzungen

Folgende Hardware und Software wird benötigt:

- externer USB SDHC Card Reader. PC-interne SDHC Card Reader werden nicht unterstützt.
- bei SDHC-Kartentausch: freigegebene SDHC-Karte.
- Image tar-Datei mit aktueller Kommunikationssoftware
- Card Manager Datei:
  - Alternative 1 - Card Manager jar-Datei: diese Java-Anwendung lässt sich direkt von einem Linux-PC oder einem Linux-PC in virtueller Umgebung starten.
  - Alternative 2 - Card Manager iso-Datei: aus dieser Datei lässt sich eine Linux-Boot-DVD brennen, die den Card Manager nach dem Booten des Linux-Systems automatisch startet.

24.8.9.1 Wie Sie mit dem Card Manager die Kommunikationssoftware auf die SDHC-Karte schreiben

Voraussetzungen

- Eine aktuelle Image-Datei ist als tar-Datei vorhanden. Die freigegebene SDHC-Karte und ein dazugehöriger USB SDHC Card Reader sind vorhanden.
- Der Schreibschutz der SDHC-Karte ist deaktiviert.
- Card Manager über Linux-Boot-DVD: die aktuelle Card Manager iso-Datei ist vorhanden, ein Admin-PC mit Windows-Betriebssystem ist vorhanden.
- Card-Manager über Java-Anwendung: die aktuelle Card Manager jar-Datei ist vorhanden, ein Linux-PC ist vorhanden.
- Das Kommunikationssystem ist ausgeschaltet und die SDHC-Karte gezogen.

Schritt für Schritt

1) Wenn Sie den Card Manager über eine Linux-Boot-DVD starten wollen:

a) Legen Sie die aktuelle Image-tar-Datei und die aktuelle Card Manager iso-Datei auf dem Admin-PC ab.

b) Erstellen Sie auf dem Admin-PC aus der aktuellen Card Manager iso-Datei eine Linux-Boot-DVD.

c) Stecken Sie den Card Reader in eine USB-Schnittstelle. Die SDHC-Karte ist nicht gesteckt!

d) Legen Sie die Linux-Boot-DVD in das DVD-Laufwerk des Admin-PC und booten Sie von DVD. Das Linux-Betriebssystem wird geladen und der Card Manager automatisch gestartet.

2) Wenn Sie den Card Manager über die Java-Anwendung starten wollen:

a) Legen Sie die aktuelle Image-tar-Datei und die aktuelle Card Manager jar-Datei auf dem Desktop des Linux-PC ab.

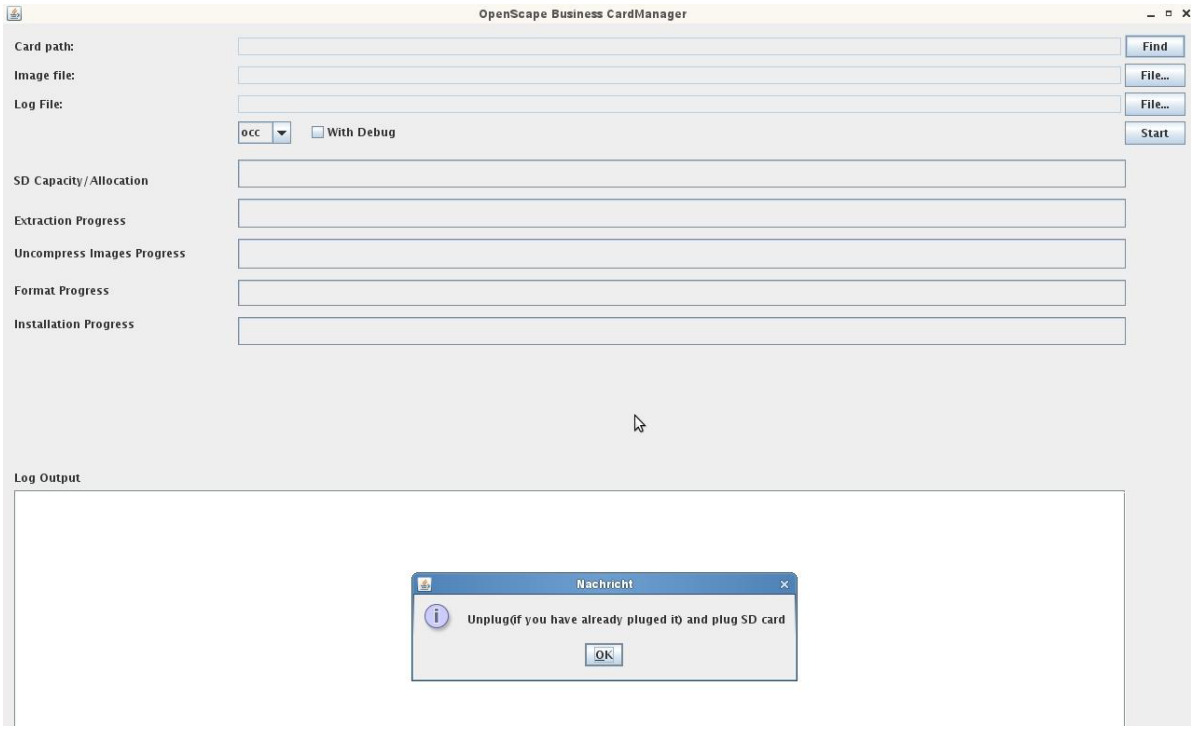
b) Klicken Sie mit der rechten Maustaste auf den Desktop und starten Sie ein neues Terminal.

c) Starten Sie den Card Manager, indem Sie im Terminal folgenden Befehl eingeben:

```
java -jar ./<Pfad_zum_Desktop>/<CardManagerFi-
leName>.jar
```

3) Wählen Sie im Card Manager aus der Aufklappliste den Eintrag **OCC** aus für das Beschreiben der SDHC-Karte.

4) Klicken Sie auf **Find**. Es erscheint folgende Meldung:



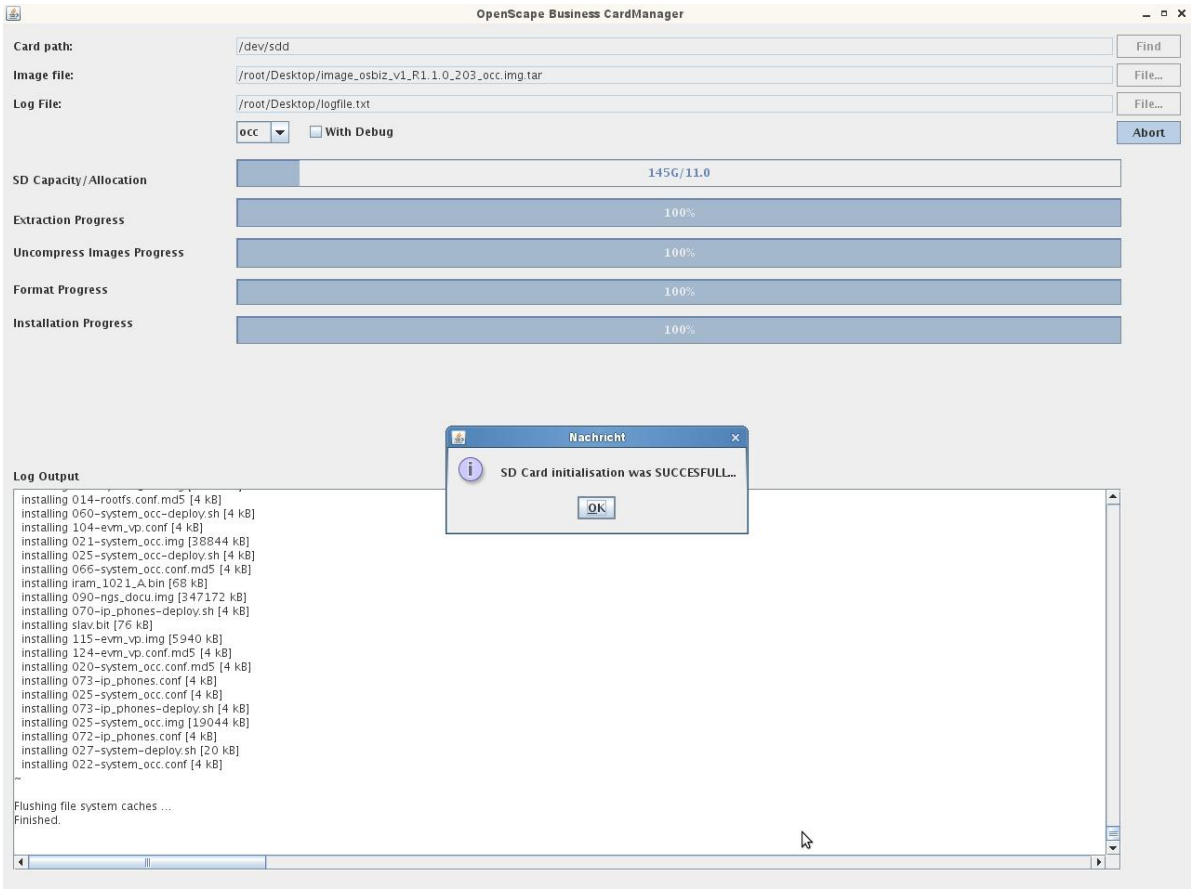
5) Stecken Sie die SDHC-Karte in den Card Reader und bestätigen Sie die Meldung mit **OK**. Unter **Card path** wird der Pfad zur SDHC-Karte angezeigt.

6) Klicken Sie bei **Image file** auf **File...** und wählen Sie die auf dem Desktop abgelegte Image-tar-Datei aus. Unter **Image file** wird der Pfad zur Image-tar-Datei angezeigt.

7) Optional können Sie auch eine Log-Datei erstellen lassen, in der eventuell aufgetretene Programmfehler aufgezeichnet werden. Klicken Sie dazu bei **Log File** auf **File...** und navigieren Sie zum Ablageort der Log-Datei. Vergeben Sie einen Namen für die Log-Datei und bestätigen Sie mit **Speichern**. Unter **Log File** wird der Pfad zur Log-Datei angezeigt.

8) Klicken Sie auf **Start**. Der Schreibvorgang wird gestartet. Der Fortschritt der einzelnen Schritte wird Ihnen über Verlaufsbalken angezeigt. Nach

Beendigung des erfolgreichen Schreibvorgangs erscheint die Meldung **SD Card initialisation was SUCCESSFULL**.



9) Bestätigen Sie die Meldung mit **OK** und entfernen Sie die SDHC-Karte aus dem Card Reader.

10) Schließen Sie den Card Manager über das X-Symbol am Fensterrand rechts oben.

11) Nur bei Card Manager über Linux-Boot-DVD: drücken Sie kurz die AN-/AUS-Taste am Admin-PC, bestätigen Sie die Meldung mit **Yes** und entnehmen Sie, sobald Sie dazu aufgefordert werden, die DVD aus dem DVD-Laufwerk.

12) Ziehen Sie den Card Reader aus der USB-Schnittstelle.

13) Stecken Sie die SDHC-Karte in den SD-Slot des ausgeschalteten Kommunikationssystems.

14) Schalten Sie das Kommunikationssystem ein. Das System ist wieder betriebsbereit, wenn die grüne LED im 1Hz-Takt blinkt (0,5s an / 0,5s aus).

INFO: Das System ist mit den Standardwerten hochgefahren, u.a. mit der Standard-IP-Adresse `192.168.1.2`.

---

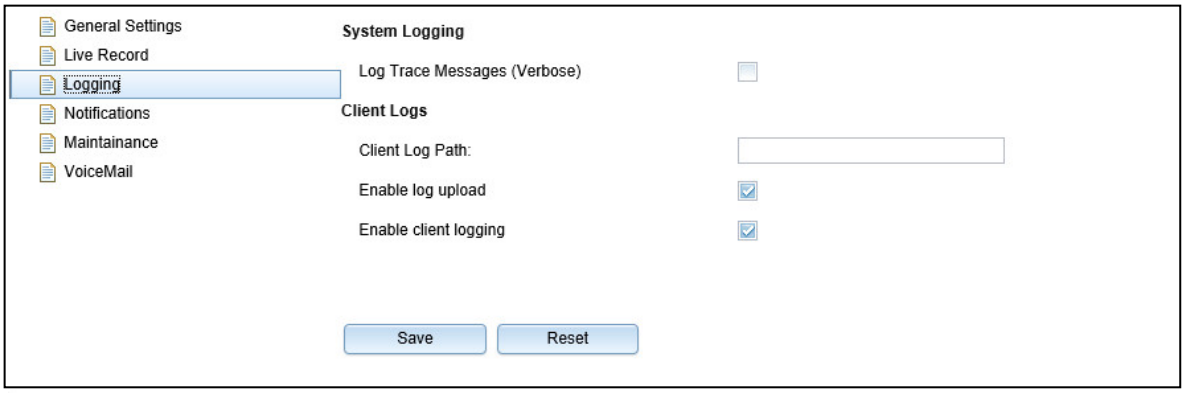
15) Führen Sie die Erstinstallation über das WBM (`https://192.168.1.2`) durch oder stellen Sie die Systemeinstellungen und Kundendaten über ein Backup-Set (falls vorhanden) wieder her.

24.9 Überwachung und Wartung der UC Suite

Das WBM bietet einem Administrator mit dem Profil **Expert** verschiedene Funktionen zur Überwachung und Wartung der UC Suite.

24.9.1 Protokollierung

Der Programmablauf der UC Suite wird systemintern überwacht. Anhand der **Systemprotokolle** kann eingestellt werden, ob eine Aufzeichnung erfolgen soll. Darüber hinaus erfolgt eine Protokollierung der Aktivitäten der UC Suite (zum Beispiel der Start eines UC Suite Clients) in **Client Logs**.



Systemprotokolle

Folgendes Systemprotokoll kann aktiviert oder deaktiviert werden:

Systemprotokoll	Standardeinstellung
Trace-Meldungen protokollieren (ausführlich)	Nicht aktiviert

Die Ergebnisse des aktivierten Systemprotokolls wird täglich in eine Protokolldatei mit der Bezeichnung `vs-jjjj-mm-tt.log` (zum Beispiel `vs-2013-01-222.log`) eingetragen und im Kommunikationssystem unter `/var/system/trace_log/vsl/log` abgelegt.

INFO: Die Auswertung der Protokolldateien ist ausschließlich durch die Entwicklung möglich.

Client Logs

Client Logs sind die Protokolldateien der UC Suite. Für jeden UC Suite Client (myPortal for Desktop, myAttendant usw.) und jeden Teilnehmer (Anwender) wird ein eigenes Verzeichnis angelegt in das die jeweiligen Protokolldateien abgelegt werden. Protokolliert werden darin die Aktivitäten eines Teilnehmers, wie beispielsweise der Start des Clients, gehende und kommende Anrufe.

> ***INFO:*** Das Ablegen von Client Logs wird ausschließlich für die UC Suite Clients unterstützt, die mit Microsoft Windows Bertriebssystemen verwendet werden.

Definiert werden kann der Pfad, in dem das Verzeichnis `CC-Logs` mit den Unterverzeichnissen der einzelnen UC Suite Clients abgelegt werden soll. Dabei kann gewählt werden, ob das Verzeichnis auf jedem Client-PC oder auf einem zentralen, im Netz befindlichen PC oder Server abgelegt werden soll.

Standardmäßig wird das Verzeichnis `CC-Logs` in folgendem Pfad abgelegt: `<Laufwerk>:\Documents and Settings/<PC-Benutzername>/CC-Logs`

Die Aufbewahrungszeit für **Client Logs** beträgt 5 Tage. Eine Änderung ist nicht möglich.

Standardmäßig ist die Protokollierung der UC Suite-Aktivitäten in **Client Logs** aktiviert. Ein Administrator mit dem Profil **Advanced** kann über den Wizard **Benutzerverzeichnis** die Protokollierung teilnehmerindividuell deaktivieren. Ein Administrator mit dem Profil **Expert** kann über den **Experten-Modus** die Protokollierung systemweit deaktivieren.

In Abhängigkeit vom Szenario werden die Client-Logs standardmäßig auch auf der Festplatte der UC Booster Card (OCAB), des UC Booster Servers oder des Kommunikationssystems OpenScape Business S abgelegt. Ein Administrator mit dem Profil **Expert** kann über den **Experten-Modus** das Speichern der Client-Logs auf der Festplatte deaktivieren.

Ein Administrator mit dem Profil **Advanced** kann über den Wizard **Trace** die Client Logs (Protokolldateien) der durch interne Teilnehmer genutzten UC Suite Clients (myPortal for Desktop, myAttendant usw.) herunterladen.

Ein Administrator mit dem Profil **Expert** kann über den **Experten-Modus** die Client Logs (Protokolldateien) der durch interne Teilnehmer genutzten UC Suite Clients (myPortal for Desktop, myAttendant usw.) herunterladen.

24.9.1.1 Wie Sie die Aufzeichnung der Systemprotokolle aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen > OpenScape Business UC Suite**.
3) Klicken Sie auf **Server** und anschließend auf **Protokolle**.
4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Trace-Meldungen täglich in einer Protokolldatei aufgezeichnet werden sollen, aktivieren Sie das Kontrollkästchen **Trace-Meldungen protokollieren (ausführlich)**.
   - Wenn Trace-Meldungen nicht in einer Protokolldatei aufgezeichnet werden sollen, deaktivieren Sie das Kontrollkästchen **Trace-Meldungen protokollieren (ausführlich)**.
5) Klicken Sie auf **Speichern**.

24.9.1.2 Wie Sie die Aufzeichnung der Client-Logs systemweit aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen > OpenScape Business UC Suite**.
3) Klicken Sie auf **Server** und anschließend auf **Protokolle**.
4) Wählen Sie eine der folgenden Möglichkeiten:
   - Wenn Client-Logs aufgezeichnet werden sollen, aktivieren Sie das Kontrollkästchen **Client-Protokollierung aktivieren**.
   - Wenn Client-Logs nicht aufgezeichnet werden sollen, deaktivieren Sie das Kontrollkästchen **Client-Protokollierung aktivieren**.

   INFO: Die Aufzeichnung von Client Logs wird ausschließlich für die UC Suite Clients unterstützt, die mit Microsoft Windows Bertriebssystemen verwendet werden.

5) Klicken Sie auf **Speichern**.

24.9.1.3 Wie Sie die Aufzeichnung der Client-Logs teilnehmerindividuell aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.

2) Klicken Sie im Navigationsbaum auf **Wizards > UC Suite**.

3) Klicken Sie auf **Bearbeiten**, um den Wizard **Benutzerverzeichnis** zu starten.

4) Markieren Sie den gewünschten Teilnehmer im Benutzerverzeichnis und klicken Sie auf **Bearbeiten**.

5) Klicken Sie im Menübaum auf **Meine Einstellungen > Verschiedenes**.

6) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Client-Logs für den gewünschten Teilnehmer aufgezeichnet werden sollen, aktivieren Sie das Kontrollkästchen **Debug-Meldungen protokollieren (ausführlich)**.
- Wenn Client-Logs für den gewünschten Teilnehmer nicht aufgezeichnet werden sollen, deaktivieren Sie das Kontrollkästchen **Debug-Meldungen protokollieren (ausführlich)**.

INFO: Die Aufzeichnung von Client Logs wird ausschließlich für die UC Suite Clients unterstützt, die mit Microsoft Windows Bertriebssystemen verwendet werden.

---

7) Klicken Sie auf **Speichern**.

8) Wenn Sie für einen weiteren Teilnehmer die Aufzeichnung der Client-Logs aktivieren oder deaktivieren möchten, wiederholen Sie die Schritte 4 bis 7.

24.9.1.4 Wie Sie den Ablagepfad für Client-Log-Dateien konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Applikationen > OpenScape Business UC Suite**.

3) Klicken Sie auf **Server** und anschließend auf **Protokolle**.

4) Geben Sie im Feld **Client-Log-Pfad** den Ablagepfad ein, in dem das Verzeichnis `CC-Logs` mit den Unterverzeichnissen der einzelnen UC Suite Clients und deren Client-Log-Dateien abgelegt werden soll. Wählen Sie eine der folgenden Möglichkeiten:

- Wenn das Verzeichnis `CC-Logs` auf jedem Client-PC abgelegt werden soll, geben Sie beispielsweise `<Laufwerk>:\<Pfad>` ein.
- Wenn das Verzeichnis `CC-Logs` auf einem zentralen, im Netz befindlichen PC oder Server abgelegt werden soll, geben Sie beispielsweise `\\<IP-Adresse>\<Laufwerk>\<Pfad>` ein.

INFO: Das Ablegen von Client Logs wird ausschließlich für die UC Suite Clients unterstützt, die mit Microsoft Windows Bertriebssystemen verwendet werden.

---

5) Klicken Sie auf **Speichern**.

24.9.1.5 Wie Sie das zentrale Speichern der Client-Logs auf der Festplatte aktivieren oder deaktivieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Applikationen > OpenScape Business UC Suite**.

3) Klicken Sie auf **Server** und anschließend auf **Protokolle**.

4) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Client-Logs auf der Festplatte der UC Booster Card (OCAB), des UC Booster Servers oder des Kommunikationssystems OpenScape Business S abgelegt werden sollen, aktivieren Sie das Kontrollkästchen **Protokoll-Upload aktivieren**.
- Wenn Client-Logs nicht auf der Festplatte der UC Booster Card (OCAB), des UC Booster Servers oder des Kommunikationssystems OpenScape Business S abgelegt werden sollen, deaktivieren Sie das Kontrollkästchen **Protokoll-Upload aktivieren**.

INFO: Die Aufzeichnung von Client Logs wird ausschließlich für die UC Suite Clients unterstützt, die mit Microsoft Windows Bertriebssystemen verwendet werden.

---

5) Klicken Sie auf **Speichern**.

24.9.1.6 Wie Sie Client Logs aller internen Teilnehmer herunterladen

Mit dem Wizard **Trace** können Sie Client Logs (Protokolldateien) der durch interne Teilnehmer genutzten UC Suite Clients (myPortal for Desktop, myAttendant usw.) herunterladen. Client Logs werden ausschließlich für die UC Suite Clients unterstützt, die mit Microsoft Windows Bertriebssystemen verwendet werden.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Diagnose > Trace**.

3) Klicken Sie auf **Diagnosedaten**.

4) Klicken Sie auf **Kein Protokoll**, um die Kontrollkästchen aller Protokolle zu deaktivieren.

5) Aktivieren Sie das Kontrollkästchen **Applikationsprotokolle**.

6) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie das gesamte vorhandene Protokoll herunterladen möchten, wählen Sie in der Aufklappliste **Gesamtes Protokoll** aus.
- Wenn Sie das Protokoll des heutigen Tages herunterladen möchten, wählen Sie in der Aufklappliste **Protokoll von heute** aus.
- Wenn Sie das Protokoll eines bestimmten Zeitraums herunterladen möchten, wählen Sie in der Aufklappliste **Eigene Auswahl** aus. Wählen Sie in der Aufklappliste **Von:** den Anfang und in der Aufklappliste **Bis:** das Ende des gewünschten Zeitraums aus.

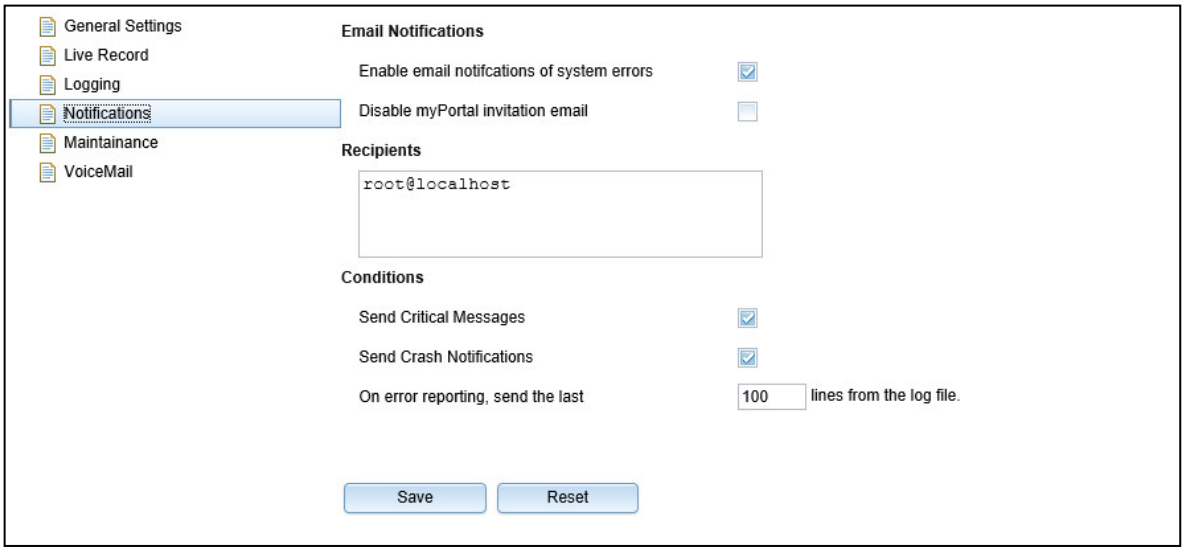
7) Klicken Sie auf **Laden** und anschließend auf **OK**. Es erscheint das Dateidownload-Fenster.

8) Speichern Sie die Datei im gewünschten Verzeichnis. Schließen Sie anschließend das Fenster, das den Download der Datei bestätigt.

9) Klicken Sie auf **Weiter** und anschließend auf **Beenden**.

24.9.2 Benachrichtigung

Durch die **E-Mail-Benachrichtigung** können E-Mails verschickt werden, um den oder die eingetragenen **Empfänger** zum Beispiel vor einem kritischem Füllstand der Festplatte zu warnen oder über Fehler zu informieren.



Das Verschicken von E-Mails kann an folgende **Bedingungen** geknüpft werden:

Bedingungen	Standardeinstellung
Wichtige Benachrichtigungen senden	Aktiviert
Benachrichtigungen über Systemabsturz senden	Aktiviert

Wichtige Benachrichtigungen und Benachrichtigungen über Systemabstürze sollten aktiviert und damit versendet werden. Diese warnen den oder die eingetragenen Empfänger über ein mögliches Problem, das an den zuständigen Service-Support gemeldet werden muss.

Zusätzlich kann definiert werden, wieviele der letzten Zeilen einer Protokolldatei mit der E-Mail verschickt werden sollen. Gemeldet werden können folgende Systemfehler (ausschließlich Englisch):

Systemfehler
NULL monitor
Could not notify CallHandler
Terminate call failed
Unable to load VM Structure from file
Alsa stuck
Alsa cancel failed
MEN CallID 0
NULL alsa handle
Database connection failed
Rules engine logic failure
Config schema format failure
90% Disk usage mark

Systemfehler
Main: Could not connect to the database !
Main: Could not load the configuration from the database!
Main: Could not open configuration file !
Main: Could not read the settings from the configuration file !
A segmentation fault was detected.
Database logic error
Database schema error
ConnectionServer failed to start
MultisiteSync failed to start
Multisite failed to start
TransferManager failed to start
IPC failed to start
ConferenceManager failed to start
CallManager failed to start
MediaProcessing failed to start
Queues failed to start
Import failed to start
DataClient failed to start
DirectoryClient failed to start
DirectoryServer failed to start
FV failed to start
IM failed to start
Switch failed to start
No Switches
Exchange Integration failed to start
Outbound Fax failed to start
SQL connection pool failed to start
Task scheduler failed to start
Trunks failed to start
Unknown switch type
Users failed to start
MEB has been disconnected
MEB ACK timeout
Switch Hearbeat timeout

24.9.2.1 Wie Sie E-Mail-Benachrichtigungen bei Systemfehlern konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Applikationen > OpenScape Business UC Suite**.

3) Klicken Sie auf **Server** und anschließend auf **Benachrichtigungen**.

4) Wählen Sie die gewünschte Einstellung für die E-Mail-Benachrichtigung aus:

- Wenn Sie eine E-Mail-Benachrichtigung möchten, aktivieren Sie das Kontrollkästchen **E-Mail-Benachrichtigungen bei Systemfehlern aktivieren**.
- Wenn Sie keine E-Mail-Benachrichtigung möchten, deaktivieren Sie das Kontrollkästchen **E-Mail-Benachrichtigungen bei Systemfehlern aktivieren**.

5) Geben Sie im Feld **Empfänger** die E-Mail-Adressen ein, an die die E-Mail-Benachrichtigungen verschickt werden sollen. Schließen Sie die Eingabe jeder E-Mail-Adresse durch Drücken von Enter ab, so dass jede E-Mail-Adresse in einer eigenen Zeile steht.

6) Wählen Sie die gewünschte Einstellung für wichtige Benachrichtigungen aus:

- Wenn Sie eine E-Mail-Benachrichtigung bei wichtigen Benachrichtigungen möchten, aktivieren Sie das Kontrollkästchen **Wichtige Benachrichtigungen senden**.
- Wenn Sie keine E-Mail-Benachrichtigung bei wichtigen Benachrichtigungen möchten, deaktivieren Sie das Kontrollkästchen **Wichtige Benachrichtigungen senden**.

7) Wählen Sie die gewünschte Einstellung für Benachrichtigungen über Systemabstürze aus:

- Wenn Sie eine E-Mail-Benachrichtigung bei Systemabstürzen möchten, aktivieren Sie das Kontrollkästchen **Benachrichtigungen über Systemabsturz senden**.
- Wenn Sie keine E-Mail-Benachrichtigung bei Systemabstürzen möchten, deaktivieren Sie das Kontrollkästchen **Benachrichtigungen über Systemabsturz senden**.

8) Geben Sie im Feld **Zeilen der Protokolldatei senden** die Anzahl der Zeilen einer Protokolldatei ein, die mit einer E-Mail verschickt werden sollen.

9) Klicken Sie auf **Speichern**.

24.9.3 Wartung

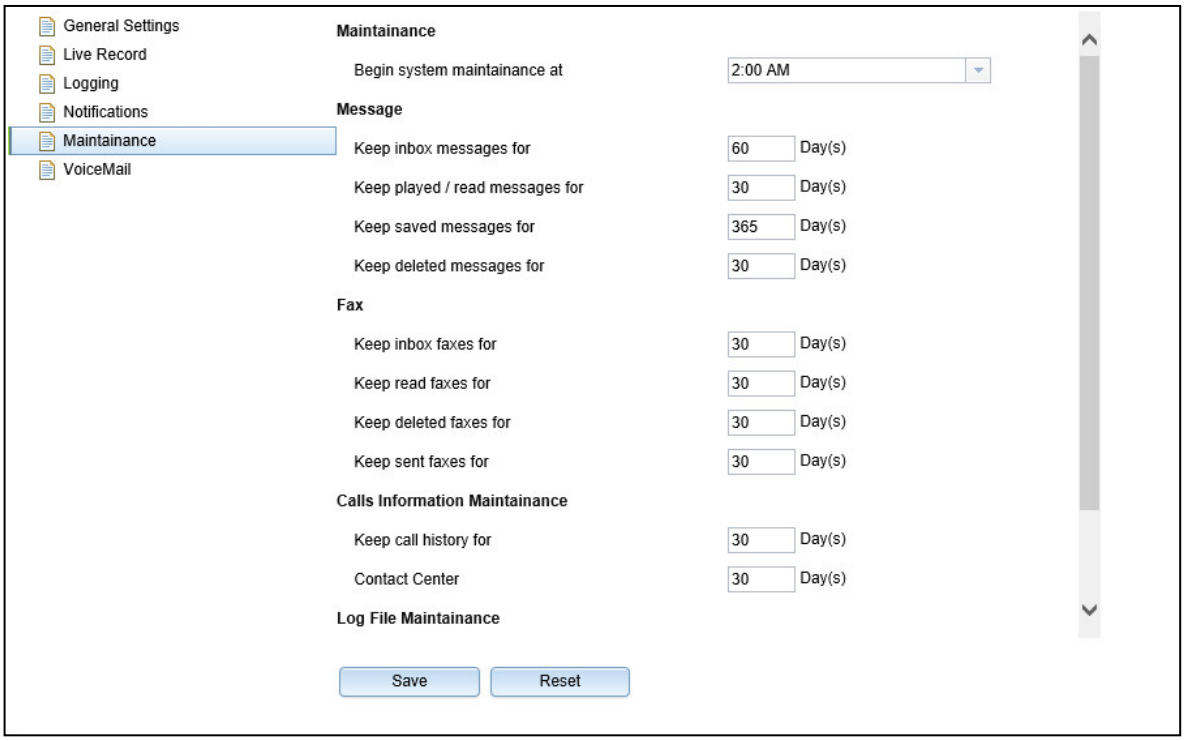
Über die Wartung können Aufbewahrungszeiten für Nachrichten, für Anrufinformationen im Anrufjournal, für die mit myAgent aufgezeichneten Anrufe, für die empfangenen und gesendeten Faxe und E-Mails für das Contact Center und für Protokolldateien definiert werden.

Ebenfalls kann eingestellt werden, zu welcher täglichen Uhrzeit das Löschen folgender Daten erfolgt, die die jeweils eingestellten Aufbewahrungszeiten überschritten haben:

- Nachrichten
- Anrufinformationen im Anrufjournal (Anrufhistorie)
- Mit myAgent aufgezeichnete Anrufe (Contact Center)
- Empfangene und gesendete Faxe und E-Mails für das Contact Center
- Protokolldateien

Die Standardeinstellung ist 2:00 Uhr.

Darüber hinaus besteht die Möglichkeit, die Systemwartung sofort zu starten und damit das sofortige Löschen der genannten Daten zu veranlassen, die die jeweils eingestellten Aufbewahrungszeiten überschritten haben. Dies kann beispielsweise notwendig sein, wenn die Festplatte des Kommunikationssystems einen kritischem Füllstand erreicht hat.



Informationen zur Wartung der Nachrichten siehe *Sprachbox (UC Suite)*.

Informationen zur **Wartung der Faxnachrichten** siehe *Administratordokumentation, UC Suite*.

Informationen zur Wartung der Anrufinformationen: Anrufhistorie siehe *Journal (UC Suite)*.

Bei der **Wartung der Anrufinformationen**: **Contact Center** werden die mit myAgent aufgezeichnete Anrufe und die empfangenen und gesendeten Faxe und E-Mails für das Contact Center gelöscht, die die eingestellte Aufbewahrungszeit überschritten haben. Die Standardeinstellung für die Aufbewahrungszeit der Contact-Center-Daten ist 60 Tage.

INFO: Die Aufbewahrungszeiten für die Wartung der Anrufinformationen sind unabhängig voneinander.

Contact-Center-Berichte basieren auf der Anrufhistorie. Wurde für die Anrufhistorie eine kürzere Aufbewahrungszeit als für die Contact-Center-Daten eingestellt, stehen einige Berichte eventuell nicht mehr zur Verfügung.

Bei der **Wartung der Protokolldateien** werden die Protokolldateien gelöscht, die die eingestellte Aufbewahrungszeit überschritten haben. Die Standardeinstellung für die Aufbewahrungszeit der Protokolldateien ist 10 Tage.

24.9.3.1 Wie Sie die Tageszeit für die Wartung konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen > OpenScape Business UC Suite**.
3) Klicken Sie auf **Server** und anschließend auf **Wartung**.
4) Geben Sie im Feld **Systemwartung beginnen um** die Uhrzeit ein, zu der die tägliche Wartung durchgeführt werden soll. Zu der hier eingestellten Uhrzeit beginnt das Löschen der Nachrichten, Anrufinformationen im Anrufjournal und Protokolldateien, die die jeweils eingestellten Aufbewahrungszeiten überschritten haben.
5) Klicken Sie auf **Speichern**.

24.9.3.2 Wie Sie die Aufbewahrungszeit für Protokolldateien konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen > OpenScape Business UC Suite**.
3) Klicken Sie auf **Server** und anschließend auf **Wartung**.
4) Geben Sie im Feld **Protokollinformationen aufbewahren für** die Aufbewahrungszeit in Tagen ein. Protokolldateien werden gelöscht, wenn diese die hier eingestellte Aufbewahrungszeit überschritten haben.
5) Klicken Sie auf **Speichern**.

24.9.3.3 Wie Sie eine sofortige Systemwartung durchführen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen > OpenScape Business UC Suite**.
3) Klicken Sie auf **Server** und anschließend auf **Wartung**.
4) Klicken Sie auf **Jetzt leeren**.

> ***INFO:*** Gelöscht werden die Nachrichten, die Anrufinformationen im Anrufjournal, die mit myAgent aufgezeichneten Anrufe, die empfangenen und gesendeten Faxe und E-Mails für das Contact Center und die Protokolldateien, die die eingestellten Aufbewahrungszeiten überschritten haben.

5) Klicken Sie auf **OK**, um das Löschen zu bestätigen.

24.9.3.4 Wie Sie die Aufbewahrungszeit für Contact-Center-Daten konfigurieren

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.
2) Klicken Sie im Navigationsbaum auf **Applikationen > OpenScape Business UC Suite**.
3) Klicken Sie auf **Server** und anschließend auf **Wartung**.

4) Geben Sie im Feld **Contact Center** die Aufbewahrungszeit in Tagen ein. Die mit myAgent aufgezeichneten Anrufe und die empfangenen und gesendeten Faxe und E-Mails für das Contact Center werden gelöscht, wenn diese die hier eingestellte Aufbewahrungszeit überschritten haben.

5) Klicken Sie auf **Speichern**.

24.10 Überwachung der UC Smart

Den aktuellen Status der UC Smart kann ein Administrator mit dem Profil **Expert** über das WBM abrufen.

24.10.1 Wie Sie den aktuellen Status der UC Smart abrufen

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

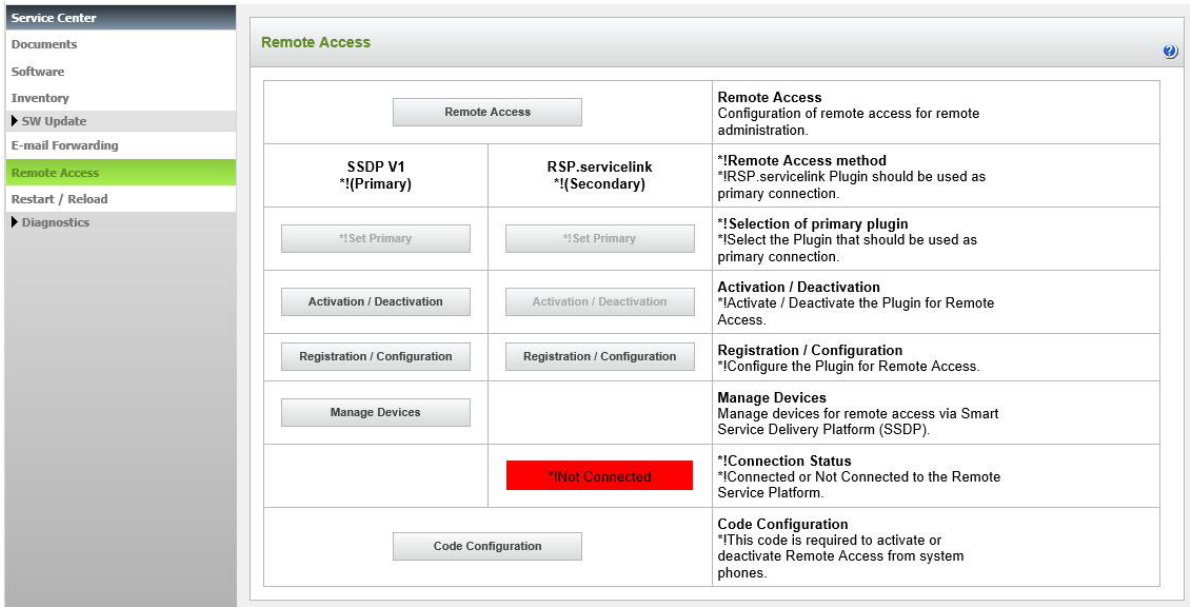
2) Klicken Sie im Navigationsbaum auf **Applikationen > UC Smart**.

3) Klicken Sie auf **Status**.

Angezeigt wird der aktuelle Status des Applikationsservers und die Anzahl der aktiven Verbindungen der einzelnen UC Clients.

24.11 Remote Services

Durch verschiedene Remote Services wird ein Fernzugriff auf das Kommunikationssystem und auf angeschlossene Komponenten durch autorisierte Servicetechniker ermöglicht. Dadurch können Wartungstätigkeiten kostengünstig durchgeführt und Anwender vor Ort bei der Lösung von Problemen unterstützt werden.



Aufgrund der hohen Bandbreite und dem Höchstmaß an Sicherheit ist der Remote Service über RSP.servicelink oder SSDP V1 zu bevorzugen (siehe RSP.servicelink und SSDP V1).

24.11.1 RSP.servicelink und SSDP V1

RSP.servicelink (**R**emote **S**ervice **P**latform) und SSDP V1 (**S**mart **S**ervices **D**elivery **P**latform) bieten autorisierten Servicetechniker eines Remote Service Partners die Möglichkeit, das Kommunikationssystem inkl. der UC Booster Applikationen bequem und sicher aus der Ferne zu administrieren. Dafür sind nur ein Internet-Anschluss, ein Webbrowser und die Partner ID des Remote Service Partners nötig. Bei RSP.servicelink wird zusätzlich ein Partner-Passwort benötigt. RSP.servicelink und SSDP V1 gewährleisten eine hohe Bandbreite und höchste Sicherheit.

RSP.servicelink ist die Weiterentwicklung von SSDP V1 und basiert auf der OpenVPN Technologie. Es nutzt SSL/TSL-Protokoll und -Verschlüsselung und bietet mit einem zusätzlichen Client-Zertifikat höchste Sicherheit. SSDP V1 wird noch eine zeitlang unterstützt, aber RSP.servicelink sollte der bevorzugte Remote-Service sein. Die Bezeichnung RSP.servicelink/SSDP V1 wird in der Dokumentation mit RSP/SSDP abgekürzt.

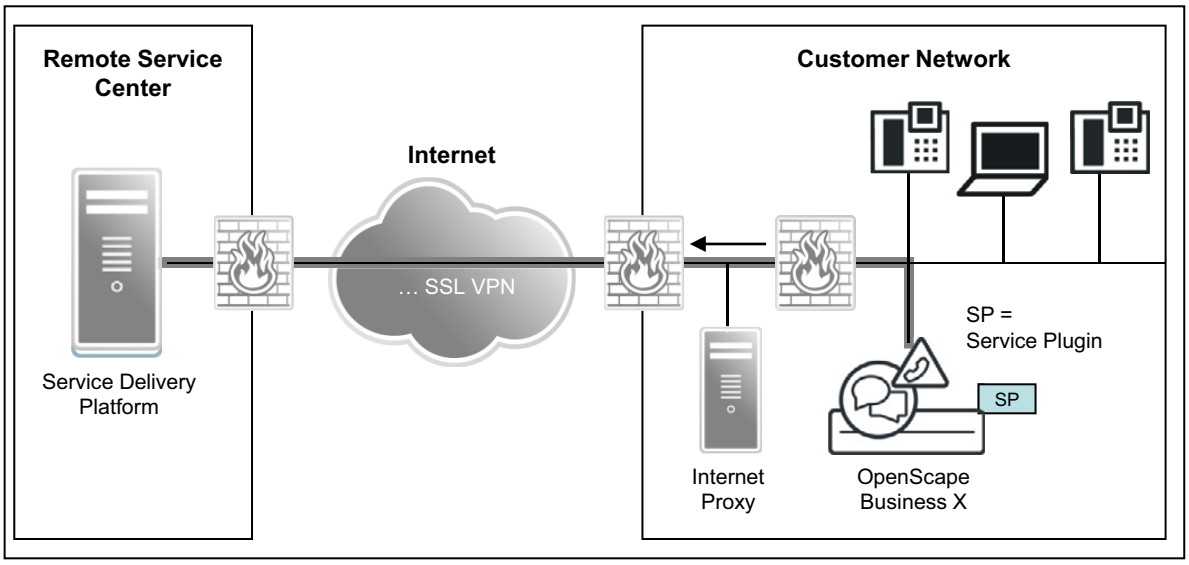
In Verbindung mit OpenScape Business bietet RSP/SSDP folgende wesentlichen Vorteile:

- Höchste Sicherheit durch gehende Internetverbindung
  Der komplette Remote-Verbindungsaufbau wird immer durch das Kommunikationssystem initiiert. Das bedeutet, die Firewall des Kundennetzes muss lediglich eine HTTPS-Verbindung zu einer einzigen Adresse im Remote Service Center zulassen (Port 443). Im Normalfall ist keine Änderung der Sicherheitsrichtlinie (Security Policy) des Kunden bzw. seiner Firewall erfor-

derlich, da dieser Port in der Firewall des Kunden in der Regel schon geöffnet ist. Damit ist eine hohe Sicherheit für das Kundennetz garantiert.
Mit RSP/SSDP behält der Administrator des Kommunikationssystems die Kontrolle über die Remote-Verbindung durch einfaches Ein- und Ausschalten des Zugangs. Bei RSP.servicelink wird zusätzlich automatisch ein Client-Zertifikat installiert.

- Hohe Bandbreite
  Durch die breitbandige Internetverbindung können im Fehlerfall Diagnosedaten schneller übertragen und damit die Servicequalität gesteigert werden.
- Einfache und kostengünstige Einrichtung
  Die Software des Kommunikationssystems beinhaltet bereits sogenannte Service Plugins für RSP.servicelink und SSDP V1. Bei der Aktivierung des Service Plugin wird die Partner ID des Remote Service Partners (und bei RSP.servicelink zusätzlich das Partner-Passwort) eingegeben.
  Jeder Remote Service Partner, der RSP.servicelink oder SSDP V1 nutzt, hat eine eigene Partner ID. Mit der vorbelegten Partner ID "Unify" kann der Fernzugriff durch autorisiertes Servicepersonal des Herstellers aktiviert werden.
- Zukunftssicherheit
  RSP/SSDP ist die Basis für zukünftige Services ("value-added" Services), wie zum Beispiel Automatisierung von Backups, Reporting und Monitoring.

Bild: RSP/SSDP – Übersicht für OpenScape Business X



RSP/SSDP unterstützt die Web Services Standards, inklusive Hypertext Transfer Protocol (HTTP), Simple Object Access Protocol (SOAP) und Extensible Markup Language (XML).

Die Kommunikation zwischen Kundenseite und Remote Service Center wird für RSP.servicelink immer mit einer AES-256-CBC-Verschlüsselung und für SSDP immer mit einer 128-Bit-SSL-Verschlüsselung abgesichert.

Service-Plugins

Für die Services RSP.servicelink und SSDP V1 gibt es jeweils eigene Service-Plugins, die einzeln aktiviert oder deaktiviert werden können.

Ein Zurücksetzen der Service-Plugins ist zum Beispiel nach dem Austausch des Mainboards erforderlich. Durch das Zurücksetzen wird die gesamte RSP- bzw. SSDP-Konfiguration gelöscht und das Service-Plugin deaktiviert.

Geräteverwaltung (Managed Device / SPoA Device)

Bei SSDP V1 kann bei Kommunikationssystemen ohne UC Booster über die Geräteverwaltung der Fernzugriff für weitere Geräte (zum Beispiel Xpressions Compact) im Kunden-LAN ermöglicht werden (Managed Device).

> ***INFO:*** Der Fernzugriff auf andere im Kunden-LAN befindliche Kommunikationssysteme OpenScape Business ist nicht möglich.

Bei RSP entspricht dem Managed Device das sogenannte SPoA Device (Single Point of Access). Die Konfiguration des SPoA Device erfolgt auf SIRA-Seite.

Aktivierung/Deaktivierung

Es bestehen folgende Möglichkeiten zur Aktivierung/Deaktivierung der Service-Plugins:

- über Wizard **Aktivierung / Deaktivierung**
  Für die Service-Plugins RSP.servicelink und SSDP V1 gibt es jeweils einen eigenen Wizard für die Aktivierung/Deaktivierung.
- über Kennzahleingabe am Systemtelefon (Standard: Aktivierung über *996, Deaktivierung über #996)
  Aus Sicherheitsgründen ist bei der Aktivierung und Deaktivierung über ein Systemtelefon zusätzlich zur Kennzahl eine 4-stellige PIN einzugeben. Die Konfiguration dieser PIN erfolgt im WBM des Kommunikationssystems mit dem Profil **Advanced**.
  Bei der Aktivierung wird das Service-Plugin aktiviert, dessen Service auf **Primär** gesetzt wurde. Bei der Deaktivierung werden sowohl das SSDP V1 Service-Plugin als auch das RSP Service-Plugin deaktiviert.

Voraussetzungen

- Internetzugang für das Kommunikationssystem oder den HTTP-Proxy im Kunden-LAN.
- Eventuell Firewall im Kunden-LAN freischalten für Registrar:
  - https://188.64.18.51
  - https://188.64.17.51
- Eventuell Firewall im Kunden-LAN freischalten für VPN:
  - https://188.64.18.50
  - https://188.64.17.50
- Bei der Internet-Konfiguration muss ein Default-Router angegeben werden.

24.11.1.1 Primären Remote-Service festlegen

Mit **Set Primary** können Sie entweder RSP.servicelink oder SSDP V1 als primären Remote-Service festlegen.

Voraussetzungen

- Eine funktionierende DNS-Konfiguration liegt vor.
- Ein Default-Router für den Internet-Zugang oder alternativ ein Proxy-Server im Kundennetz ist vorhanden.
- Partner ID und Partner-Passwort Ihres Remote Service Partners liegen vor (vorbelegte Partner ID: Unify).
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Remote-Zugang**.

3) Klicken Sie bei dem Remote-Service auf **Set Primary**, den Sie als primären Remote-Service festlegen wollen.

24.11.1.2 Wie Sie das RSP Service-Plugin installieren, konfigurieren und registrieren

Mit dem Wizard **Registrierung / Konfiguration** können Sie das RSP Service-Plugin für den Remote-Zugriff auf das Kommunikationssystem über RSP installieren, konfigurieren und registrieren.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Remote-Zugang**.

3) Klicken Sie auf **Registrierung / Konfiguration**.

4) Wenn das RSP Service-Plugin noch nicht installiert ist, klicken Sie auf **Installieren** und anschließend auf **OK & Weiter**.

5) Wenn das RSP Service-Plugin bereits installiert ist, klicken Sie auf **OK & Weiter**.

6) Wenn im Kundennetz kein Proxy-Server genutzt wird, klicken Sie auf **OK & Weiter**, da eine Konfiguration der **Proxy-Parameter** nicht erforderlich ist. Überspringen Sie die nächsten beiden Schritte.

7) Wenn im Kundennetz ein Proxy-Server genutzt wird, müssen Sie die Einstellung der **Proxy-Parameter** abhängig vom Kundennetz auswählen:

- Wenn im Kundennetz ein Proxy mit HTTP-Protokoll vorliegt, aktivieren Sie das Kontrollkästchen **HTTP Proxy verwenden**. Geben Sie im Feld **HTTP Proxy Host** den Hostnamen und im Feld **HTTP Proxy Port** die Portnummer des Proxy-Servers ein. Falls erforderlich, geben Sie im Feld **Benutzername** den Benutzernamen und im Feld **Passwort** das Passwort für die Authentifizierung am Proxy-Server ein.
- Wenn im Kundennetz ein Proxy mit SOCKS-Protokoll vorliegt, aktivieren Sie das Kontrollkästchen **SOCKS Proxy verwenden**. Geben Sie im Feld **SOCKS Proxy Host** den Hostnamen und im Feld **SOCKS Proxy Port** die Portnummer des Proxy-Servers ein. Falls erforderlich, geben Sie im Feld **Benutzername** den Benutzernamen und im Feld **Passwort** das Passwort für die Authentifizierung am Proxy-Server ein.

INFO: Ob eine Authentifizierung erforderlich ist oder nicht, hängt vom Typ und von der Konfiguration des Proxy-Servers ab.

---

8) Klicken Sie auf **OK & Weiter**.

9) Ändern Sie nur bei Bedarf im Feld **Partner ID** die vorbelegte Partner ID.

10) Geben Sie im Feld **Passwort** Ihr Passwort ein.

11) Klicken Sie auf **Beenden**.

In der Spalte **RSP.servicelink** wird Ihnen in der Zeile **Connection Status** angezeigt, ob die Registrierung erfolgreich war. Im Falle einer nicht erfolgreichen Registrierung können folgende Fehlermeldungen angezeigt werden:

- MAC already registered:
  Lösung: Gerät (= OpenScape Business Kommunikationssystem) auf dem SIRA-Server löschen und mit dem Wizard **Registrierung / Konfiguration** neu registrieren.

INFO: Über die MAC-Adresse finden Sie das Gerät auf dem SIRA-Server. Die MAC-Adresse des OpenScape Business Kommunikationssystems finden Sie im **Service-Center** unter **Inventory**.

- Configuration Error:
  Lösung: Im Wizard **Registrierung / Konfiguration** Partner-ID und Passwort neu eingeben und den Wizard korrekt beenden.
- Wrong Credentials:
  Lösung: Im Wizard **Registrierung / Konfiguration** Partner-ID und Passwort neu eingeben und den Wizard korrekt beenden.

24.11.1.3 Wie Sie das SSDP Service-Plugin konfigurieren und registrieren

Mit dem Wizard **Registrierung / Konfiguration** können Sie das SSDP Service-Plugin für den Remote-Zugriff auf das Kommunikationssystem über SSDP V1 konfigurieren und registrieren.

Voraussetzungen

- Das SSDP Service-Plugin ist aktiviert.
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Remote-Zugang**.

3) Klicken Sie in der Spalte **SSDP V1** auf **Registrierung / Konfiguration**.

4) Wenn im Kundennetz kein Proxy-Server genutzt wird, klicken Sie auf **OK & Weiter**, da eine Konfiguration der **Proxy-Parameter** nicht erforderlich ist. Überspringen Sie die nächsten beiden Schritte.

5) Wenn im Kundennetz ein Proxy-Server genutzt wird, müssen Sie die Einstellung der **Proxy-Parameter** abhängig vom Kundennetz auswählen:

- Wenn im Kundennetz ein Proxy mit Auto-Konfiguration vorliegt, aktivieren Sie das Kontrollkästchen **Aktivierung Proxy Auto-Konfiguration**. Geben Sie im Feld **URL** die URL des Proxy-Konfigurationsscripts ein.
- Wenn im Kundennetz ein Proxy mit HTTP-Protokoll vorliegt, aktivieren Sie das Kontrollkästchen **HTTP Proxy verwenden**. Geben Sie im Feld **HTTP Proxy Host** den Hostnamen und im Feld **HTTP Proxy Port** die Portnummer des Proxy-Servers ein. Falls erforderlich, geben Sie im Feld **Benutzername** den Benutzernamen und im Feld **Passwort** das Passwort für die Authentifizierung am Proxy-Server ein.
- Wenn im Kundennetz ein Proxy mit SOCKS-Protokoll vorliegt, aktivieren Sie das Kontrollkästchen **SOCKS Proxy verwenden**. Geben Sie im Feld **SOCKS Proxy Host** den Hostnamen und im Feld **SOCKS Proxy Port** die Portnummer des Proxy-Servers ein. Falls erforderlich, geben Sie im Feld **Benutzername** den Benutzernamen und im Feld **Passwort** das Passwort für die Authentifizierung am Proxy-Server ein.

  INFO: Ob eine Authentifizierung erforderlich ist oder nicht, hängt vom Typ und von der Konfiguration des Proxy-Servers ab.

6) Klicken Sie auf **OK & Weiter**. Das Fenster **Geräte-Identifikation** wird angezeigt.

7) Im Feld **Geräte-Modell** wird das Modell des Kommunikationssystems angezeigt. Eine Änderung dieses Wertes ist nicht möglich.

8) Im Feld **Smart Services Geräte-ID** wird die Geräte-ID des SSDP Service-Plugin angezeigt. Eine Änderung dieses Wertes ist nicht möglich.

9) Wählen Sie eine der folgenden Möglichkeiten für die Eingabe im Feld **Gerätename**:

- Wenn es sich um einen Kunden mit einem Software-Wartungsvertrag der Unify GmbH & Co. KG handelt, geben Sie im Feld **Gerätename** folgende

Daten ein: `<Systemkürzel>_<Equipmentnummer>_<Vertragsnummer>`.

Systemkürzel: OpenScape Business X3R = OSBizX3R, OpenScape Business X3W = OSBizX3W, OpenScape Business X5R = OSBizX5R, OpenScape Business X5W = OSBizX5W, OpenScape Business X8 = OSBizX8, OpenScape Business S = OSBizS, OpenScape Business UC Booster Server = OSBizUCBS

Equipmentnummer = Über GSI (Global Service Infrastructure)-Flow zu ermitteln

Vertragsnummer = Steht im Auftrag für die Installation des Kommunikationssystems

Beispiel: `OSBizX5W_1234567890_12345678`

- Wenn es sich nicht um einen Kunden mit einem Software-Wartungsvertrag der Unify GmbH & Co. KG handelt, geben Sie im Feld **Gerätename** folgende Daten ein: `<Systemkürzel>_<eindeutige Kundennummer>`.

  Systemkürzel: OpenScape Business X3R = OSBizX3R, OpenScape Business X3W = OSBizX3W, OpenScape Business X5R = OSBizX5R, OpenScape Business X5W = OSBizX5W, OpenScape Business X8 = OSBizX8, OpenScape Business S = OSBizS, OpenScape Business UC Booster Server = OSBizUCBS

  Eindeutige Kundennummer: Vertrags- oder Servicenummer, mit der der Kunde eindeutig bezeichnet werden kann.

10) Klicken Sie auf **Beenden**.

24.11.1.4 Wie Sie das RSP Service-Plugin aktivieren

Mit dem Wizard **Aktivierung / Deaktivierung** können Sie das RSP Service-Plugin für den Remote-Zugriff auf das Kommunikationssystem über RSP aktivieren.

Voraussetzungen

- Eine funktionierende DNS-Konfiguration liegt vor.
- Ein Default-Router für den Internet-Zugang oder alternativ ein Proxy-Server im Kundennetz ist vorhanden.
- Das RSP Service-Plugin ist deaktiviert.
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Remote-Zugang**.

3) Klicken Sie in der Spalte **RSP.servicelink** auf **Aktivierung / Deaktivierung**.

4) Klicken Sie auf **Aktivieren**.

24.11.1.5 Wie Sie das SSDP Service-Plugin aktivieren

Mit dem Wizard **Aktivierung / Deaktivierung** können Sie das SSDP Service-Plugin für den Remote-Zugriff auf das Kommunikationssystem über SSDP V1 aktivieren.

Voraussetzungen

- Eine funktionierende DNS-Konfiguration liegt vor.
- Ein Default-Router für den Internet-Zugang oder alternativ ein Proxy-Server im Kundennetz ist vorhanden.
- Partner ID Ihres Remote Service Partners liegen vor (vorbelegte Partner ID: Unify).
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Remote-Zugang**.

3) Klicken Sie in der Spalte **SSDP V1** auf **Aktivierung / Deaktivierung**.

4) Ändern Sie im Feld **Partner ID** bei Bedarf die vorbelegte Partner ID und klicken Sie auf **Sichern**.

5) Klicken Sie auf **Aktivieren**.

24.11.1.6 Wie Sie das Service-Plugin deaktivieren

Mit dem Wizard **Aktivierung / Deaktivierung** können Sie das SSDP Service-Plugin oder das RSP Service-Plugin für den Remote-Zugriff auf das Kommunikationssystem über RSP/SSDP deaktivieren.

Voraussetzungen

- Das SSDP Service-Plugin und/oder das RSP Service-Plugin sind aktiviert.
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Remote-Zugang**.

3) Klicken Sie in der Spalte **SSDP V1** oder in der Spalte **RSP.serivelink** auf **Aktivierung / Deaktivierung**.

4) Klicken Sie auf **Deaktivieren**.

24.11.1.7 Wie Sie das RSP Service-Plugin zurücksetzen

Mit dem Wizard **Aktivierung / Deaktivierung** können Sie das RSP Service-Plugin zurücksetzen. Damit wird die gesamte RSP-Konfiguration gelöscht und das RSP Service-Plugin deaktiviert.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Remote-Zugang**.

3) Klicken Sie in der Spalte **RSP.servicelink** auf **Aktivierung / Deaktivierung**.

4) Klicken Sie auf **Auf Standard zurücksetzen** und anschließend auf **OK**.

5) Klicken Sie in der Spalte **RSP.servicelink** auf **Aktivierung / Deaktivierung**.

6) Klicken Sie auf **Deaktivieren**.

7) Löschen Sie auf dem SIRA-Server das Gerät (= OpenScape Business Kommunikationssystem).

INFO: Über die MAC-Adresse finden Sie das Gerät auf dem SIRA-Server. Die MAC-Adresse des OpenScape Business Kommunikationssystems finden Sie im **Service-Center** unter **Inventory**.

24.11.1.8 Wie Sie das SSDP Service-Plugin zurücksetzen

Mit dem Wizard **Aktivierung / Deaktivierung** können Sie das SSDP Service-Plugin zurücksetzen. Damit wird die gesamte SSDP-Konfiguration gelöscht und das SSDP Service-Plugin deaktiviert.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Remote-Zugang**.

3) Klicken Sie in der Spalte **SSDP V1** auf **Aktivierung / Deaktivierung**.

4) Klicken Sie auf **Auf Standard zurücksetzen** und anschließend auf **OK**.

24.11.1.9 Wie Sie die Partner ID des SSDP Service-Plugins ändern

Mit dem Wizard **Aktivierung / Deaktivierung** können Sie die Partner-ID des SSDP Service-Plugins ändern.

Voraussetzungen

- Das Service-Plugin ist aktiviert.
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Remote-Zugang**.

3) Klicken Sie in der Spalte **SSDP V1** auf **Aktivierung / Deaktivierung**.

4) Ändern Sie im Feld **Partner ID** die Partner ID.

5) Klicken Sie auf **Sichern**.

24.11.1.10 Wie Sie den Fernzugriff auf LAN-Geräte hinzufügen oder löschen (nur für SSDP)

Mit dem Wizard **Geräte verwalten** konfigurieren Sie den SSDP-Fernzugriff für Geräte im Kunden-LAN.

Voraussetzungen

- Das SSDP Service-Plugin ist aktiviert.
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Remote-Zugang**.

3) Klicken Sie auf **Geräte verwalten**, um den zugehörigen Wizard zu starten.

4) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie ein Gerät für den Fernzugriff hinzufügen möchten, gehen Sie folgendermaßen vor:

  Geben Sie im Feld **Host/IP-Adresse** den Hostnamen oder die IP-Adresse des gewünschten Gerätes ein.

  Wählen Sie in der Aufklappliste Modell das Modell des gewünschten Gerätes aus. Sie haben folgende Möglichkeiten:

– Wenn Sie die VoiceMail-Lösung Xpressions Compact für den Fernzugriff hinzufügen möchten, wählen Sie den Eintrag **Xpressions Compact** aus.

– Wenn Sie ein Gerät für den Fernzugriff hinzufügen möchten und der Fernzugriff unverschlüsselt (über HTTP-Protokoll) erfolgen soll, wählen Sie den Eintrag **DeviceHttp** aus.

– Wenn Sie ein Gerät für den Fernzugriff hinzufügen möchten und der Fernzugriff verschlüsselt (über HTTPS-Protokoll) erfolgen soll, wählen Sie den Eintrag **DeviceHttps** aus.

Geben Sie im Feld **Smart Services Geräte-ID** die Geräte-ID des Service-Plugin ein.

Klicken Sie auf **Hinzufügen**.

- Wenn Sie den Fernzugriff für ein Gerät löschen möchten, klicken Sie in der Zeile des gewünschten Gerätes auf **Löschen**.

5) Klicken Sie auf **Beenden** und anschließend auf **OK**.

Das Service-Plugin führt einen Neustart aus.

24.11.1.11 Wie Sie eine PIN für die Aktivierung und Deaktivierung des Service-Plugin konfigurieren

Die PIN gilt für die Aktivierung und die Deaktivierung des Service-Plugin über ein Systemtelefon.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Remote-Zugang**.

3) Geben Sie im Feld **PIN** die gewünschte vierstellige PIN ein.

4) Klicken Sie auf **Sichern** und anschließend auf **OK**.

Nächste Schritte

Die Aktivierung des primären Service-Plugins über ein Systemtelefon erfolgt durch Eingabe der entsprechenden Kennzahl (Standardkennzahl = *996) und anschließender Eingabe der vierstelligen PIN.

Die Deaktivierung der Service-Plugins über ein Systemtelefon erfolgt durch Eingabe der entsprechenden Kennzahl (Standardkennzahl = #996) und anschließender Eingabe der vierstelligen PIN.

24.11.2 Remote-Zugang

Durch den Remote-Zugang kann autorisierten Servicetechnikern über eine ISDN-PSTN- oder Internet-Verbindung der Fernzugriff auf die Kommunikationssysteme OpenScape Business X ermöglicht werden. Damit ist zum Beispiel die Unterstützung bei der Lösung von Administrationsaufgaben oder bei der Fehlersuche möglich.

Um den Fernzugriff auf das Kommunikationssystem zu ermöglichen, muss der Remote-Zugang eingeschaltet werden. Es bestehen folgende Zugriffsmöglichkeiten:

- Remote-Zugang über ISDN-PSTN-Verbindung

  INFO: Beim Remote-Zugang über eine ISDN-PSTN-Verbindung kann es aufgrund der begrenzten Übertragungsgeschwindigkeit zu längeren Wartezeiten kommen.

  Zur Einwahl über ISDN benötigt der Servicetechniker eine für das Kommunikationssystem gültige Durchwahlnummer (**Einwahlnummer**).
  Die UC Booster Applikationen (wie z. B. UC Suite, OpenDirectory Service, Gate View) können über diesen Remote-Zugang administriert werden, wenn die IP-Adresse des Mainboards für UC Booster als Router (z. B. Default Router) konfiguriert ist.
- Remote-Zugang über Internet-Verbindung

  INFO: Beim Remote-Zugang über eine Internet-Verbindung besteht ein erhöhtes Sicherheitsrisiko.

  Zur Einwahl über Internet benötigt der Servicetechniker einen speziellen Port (**Port-Nummer**) zum Zugriff auf das Kommunikationssystem. Standardmäßig ist die Port-Nummer 10099 eingetragen. Bei Verwendung eines externen Routers muss im externen Router eine Port-Weiterleitung für diese Port-Nummer eingerichtet werden.
  Die Port-Nummer darf nicht durch eine eventuell vorhandene Firewall auf dem PC des Servicetechnikers gesperrt sein. Die Auswahl der Port-Nummer ist deshalb mit dem Servicetechniker abzustimmen.
  Die UC Booster Applikationen (wie z. B. UC Suite, OpenDirectory Service, Gate View) können über diesen Remote-Zugang nicht administriert werden.

Um den Fernzugriff auf das Kommunikationssystem zu deaktivieren, muss der Remote-Zugang ausgeschaltet werden.

HINWEIS: Um nicht autorisierte Zugriffe auf das Kommunikationssystem zu vermeiden, ist der Remote-Zugang nach Beendigung der Fernadministration wieder auszuschalten.

Die Fernwartung des Kommunikationssystems ist darüber hinaus auch via ISDN X.75 über das Servicetool Manager E möglich. Die hierfür benötigte Zugangsrufnummer wird im Manager E unter **Digital Modem (x75)** konfiguriert.

24.11.2.1 Wie Sie den Remote-Zugang über ISDN einschalten

Mit dem Wizard **Remote-Zugang** können Sie autorisierten Servicetechnikern über eine ISDN-Verbindung den Zugriff auf das Kommunikationssystem ermöglichen.

Voraussetzungen

- OpenScape Business X verfügt über eine ISDN-Amtsverbindung.
- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Remote-Zugang**.

3) Klicken Sie auf **Remote-Zugang**, um den Wizard **Remote-Zugang** zu starten.

4) Aktivieren Sie das Optionsfeld **Remote-Zugang: ein**, um den Remote-Zugang einzuschalten.

5) Aktivieren Sie das Optionsfeld **Remote-Zugang über: ISDN**, um den Remote-Zugang über ISDN einzuschalten.

6) Geben Sie im Feld **Rufnummer** die interne Rufnummer ein, über die der Remote-Zugang erfolgen soll.

7) Geben Sie im Feld **Einwahlnummer** die Durchwahlnummer ein, über die der Remote-Zugang erfolgen soll.

8) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**.

24.11.2.2 Wie Sie einen PC mit Microsoft Windows Vista für Remote-Zugang über ISDN konfigurieren

Voraussetzungen

- Der PC ist mit einer ISDN-Karte ausgestattet und verfügt über eine ISDN-Amtsverbindung.
- Der Zugriff soll auf ein Kommunikationssystem OpenScape Business X3/X5/X8 mit Anlagenanschluss erfolgen. Ortsnetzkennzahl und Anlagenrufnummer des Kommunikationssystems liegen vor.
- Der Remote-Zugang über ISDN wurde eingeschaltet. Die Einwahlnummer für den Remote-Zugang des Kommunikationssystems liegt vor.
- Benutzername und Kennwort für den Zugriff auf das Kommunikationssystem liegen vor.

INFO: Die folgende Beschreibung bezieht sich auf einen PC mit dem Betriebssystem Microsoft Windows Vista. Ein ähnlicher Ablauf ergibt sich für das Betriebssystem Microsoft Windows XP.

Schritt für Schritt

1) Klicken Sie im **Startmenü** von Windows Vista auf **Verbindung herstellen**. Das Fenster **Verbindung mit einem Netzwerk herstellen** erscheint.

2) Klicken Sie auf **Eine Verbindung oder ein Netzwerk einrichten**.

3) Klicken Sie auf die Verbindungsoption **Verbindung mit dem Arbeitsplatz herstellen** und anschließend auf **Weiter**.

4) Klicken Sie auf **Direkt wählen**.

5) Geben Sie im Feld **Rufnummer** die Amtskennziffer (zum Beispiel `0`), die Ortsnetzkennzahl (zum Beispiel `089`), die Anlagenrufnummer (zum Beispiel `12345678`) und die Einwahlnummer (zum Beispiel `666`) ein.

Der Gesamteintrag für die genannten Beispiele lautet: `008912345678666`

6) Geben Sie im Feld **Zielname** eine Bezeichnung für diese Verbindung ein.

7) Aktivieren Sie das Kontrollkästchen **Jetzt nicht verbinden, nur für spätere Verwendung einrichten**.

8) Klicken Sie auf **Weiter**.

9) Geben Sie im Feld **Benutzername** den Benutzernamen für den Zugriff auf das Kommunikationssystem ein.

10) Geben Sie im Feld **Kennwort** das Kennwort für den Zugriff auf das Kommunikationssystem ein.

INFO: Als Standarddaten für den Zugriff auf das Kommunikationssystem werden der Standard-Benutzername und das Standard-Kennwort für den Systemzugriff mittels Servicetool Manager E verwendet.

11) Klicken Sie auf **Erstellen**.

12) Klicken Sie auf **Verbindung jetzt herstellen**.

Damit ist der Fernzugriff auf das Kommunikationssystem möglich.

INFO: Um die Verbindung zu deaktivieren, klicken Sie auf **Start > Verbindung herstellen**. Klicken Sie auf die im Schritt 6 definierte Bezeichnung der Verbindung (**Zielname**) und anschließend auf **Trennen**.

Das Aktivieren der Verbindung ist durch Klicken auf die im Schritt 6 definierte Bezeichnung (**Zielname**) und anschließendes Klicken auf **Verbinden** möglich.

24.11.2.3 Wie Sie einen PC mit Microsoft Windows 7 für Remote-Zugang über ISDN konfigurieren

Voraussetzungen

- Der PC ist mit einer ISDN-Karte ausgestattet und verfügt über eine ISDN-Amtsverbindung.
- Der Zugriff soll auf ein Kommunikationssystem OpenScape Business X3/X5/X8 mit Anlagenanschluss erfolgen. Ortsnetzkennzahl und Anlagenrufnummer des Kommunikationssystems liegen vor.
- Der Remote-Zugang über ISDN wurde eingeschaltet. Die Einwahlnummer für den Remote-Zugang des Kommunikationssystems liegt vor.
- Benutzername und Kennwort für den Zugriff auf das Kommunikationssystem liegen vor.

INFO: Die folgende Beschreibung bezieht sich auf einen PC mit dem Betriebssystem Microsoft Windows 7.

Schritt für Schritt

1) Klicken Sie im **Startmenü** von Windows 7 auf **Systemsteuerung**.

2) Klicken Sie auf **Netzwerk und Internet**.

3) Klicken Sie auf **Netzwerk- und Freigabecenter**.

4) Klicken Sie auf **Eine Verbindung oder ein Netzwerk einrichten**.

5) Klicken Sie auf die Verbindungsoption **Verbindung mit dem Arbeitsplatz herstellen** und anschließend auf **Weiter**.

6) Klicken Sie auf **Direkt wählen**.

7) Geben Sie im Feld **Rufnummer** die Amtskennziffer (zum Beispiel `0`), die Ortsnetzkennzahl (zum Beispiel `089`), die Anlagenrufnummer (zum Beispiel `12345678`) und die Einwahlnummer (zum Beispiel `666`) ein.

Der Gesamteintrag für die genannten Beispiele lautet: `008912345678666`

8) Geben Sie im Feld **Zielname** eine Bezeichnung für diese Verbindung ein.

9) Aktivieren Sie das Kontrollkästchen **Jetzt nicht verbinden, nur für spätere Verwendung einrichten**.

10) Klicken Sie auf **Weiter**.

11) Geben Sie im Feld **Benutzername** den Benutzernamen für den Zugriff auf das Kommunikationssystem ein.

12) Geben Sie im Feld **Kennwort** das Kennwort für den Zugriff auf das Kommunikationssystem ein.

INFO: Als Standarddaten für den Zugriff auf das Kommunikationssystem werden der Standard-Benutzername und das

Standard-Kennwort für den Systemzugriff mittels Servicetool Manager E verwendet.

13) Klicken Sie auf **Erstellen**.

14) Klicken Sie auf **Verbindung jetzt herstellen**. Anschließend erscheint die Meldung `Verbindung wurde hergestellt`.

15) Klicken Sie auf **Schließen**.

Damit ist der Fernzugriff auf das Kommunikationssystem möglich.

INFO: Um die Verbindung zu deaktivieren, klicken Sie in der Symbolleiste auf das Symbol **Netzwerk**. Klicken Sie auf die im Schritt 8 definierte Bezeichnung der Verbindung (**Zielname**) und anschließend auf **Trennen**.

Das Aktivieren der Verbindung ist durch Klicken auf die im Schritt 8 definierte Bezeichnung (**Zielname**) und anschließendes Klicken auf **Verbinden** möglich.

24.11.2.4 Wie Sie den Remote-Zugang über Internet-Zugang mit fester IP-Adresse einschalten

Mit dem Wizard **Remote-Zugang** können Sie autorisierten Servicetechnikern über eine Internet-Verbindung den Zugriff auf das Kommunikationssystem ermöglichen.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.
- Ihnen liegt eine Port-Nummer vor, über die der Internet-Zugriff des Servicetechnikers auf das Kommunikationssystem möglich ist. Diese Port-Nummer darf nicht durch eine eventuell vorhandene Firewall auf dem PC des Servicetechnikers gesperrt sein.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Remote-Zugang**.

3) Klicken Sie auf **Remote-Zugang**, um den Wizard **Remote-Zugang** zu starten.

4) Aktivieren Sie das Optionsfeld **Remote-Zugang: ein**, um den Remote-Zugang einzuschalten.

5) Aktivieren Sie das Optionsfeld **Remote-Zugang über: Internet**, um den Remote-Zugang über Internet einzuschalten.

6) Geben Sie im Feld **Port-Nummer** die Port-Nummer ein, über die der Remote-Zugang erfolgen soll.

Standardmäßig ist die Port-Nummer 10099 eingetragen.

7) Klicken Sie auf **OK & Weiter**. Die Meldung `Der Remote-Zugang wurde aktiviert ...` wird angezeigt. Diese Meldung enthält die URL, über die der Fernzugriff auf das Kommunikationssystem per Webbrowser möglich ist.

8) Klicken Sie auf **Beenden**.

24.11.2.5 Wie Sie den Remote-Zugang über Internet-Zugang ohne feste IP-Adresse einschalten

Mit dem Wizard **Remote-Zugang** können Sie autorisierten Servicetechnikern über eine Internet-Verbindung den Zugriff auf das Kommunikationssystem ermöglichen.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.
- Ihnen liegt eine Port-Nummer vor, über die der Internet-Zugriff des Servicetechnikers auf das Kommunikationssystem möglich ist. Diese Port-Nummer darf nicht durch eine eventuell vorhandene Firewall auf dem PC des Servicetechnikers gesperrt sein.
- Ein DynDNS-Account liegt vor.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Remote-Zugang**.

3) Klicken Sie auf **Remote-Zugang**, um den Wizard **Remote-Zugang** zu starten.

4) Aktivieren Sie das Optionsfeld **Remote-Zugang: ein**, um den Remote-Zugang einzuschalten.

5) Aktivieren Sie das Optionsfeld **Remote-Zugang über: Internet**, um den Remote-Zugang über Internet einzuschalten.

6) Geben Sie im Feld **Port-Nummer** die Port-Nummer ein, über die der Remote-Zugang erfolgen soll.

Standardmäßig ist die Port-Nummer 10099 eingetragen.

7) Klicken Sie auf **OK & Weiter**, um die Eingaben zu übernehmen. Das Fenster **DynDNS-Account einrichten** erscheint.

8) Geben Sie im Feld **Benutzername** den Benutzernamen für Ihren DynDNS-Account beim DynDNS-Anbieter ein, falls dieser nicht bereits angezeigt wird.

9) Geben Sie im Feld **Passwort** und im Feld **Passwort wiederholen** das Passwort Ihres DynDNS-Accounts beim DynDNS-Anbieter ein, falls dieses nicht bereits angezeigt wird.

10) Geben Sie im Feld **Hostname** Ihren vom DynDNS-Anbieter zugeteilten Hostnamen ohne den Domänennamen ein (zum Beispiel `myhost`), falls dieser nicht bereits angezeigt wird.

11) Wählen Sie in der Aufklappliste **Domainname** Ihren DynDNS-Anbieter aus (zum Beispiel `dyndns.org`), falls dieser nicht bereits angezeigt wird. Ihr vollständiger Domänenname lautet dann beispielsweise `myhost.dyndns.org`.

12) Klicken Sie auf **Verbindung testen**. Das Fenster **DynDNS-Zugang testen** erscheint.

13) Klicken Sie auf **OK**. Die DynDNS-Zugangsdaten werden nun zum Provider übermittelt. Das dauert ca. 10 Sekunden.

14) Wenn der Test erfolgreich war, wird die Meldung `Der Remote-Zugang wurde aktiviert ...` angezeigt. Diese Meldung enthält die URL, über die der Fernzugriff auf das Kommunikationssystem per Webbrowser möglich ist. Klicken Sie auf **Beenden**.

15) Wenn der Test nicht erfogreich war, klicken Sie auf **OK**. Im anschließend erscheinenden Fenster **DynDNS-Zugang** erhalten Sie Hinweise zu den möglichen Fehlerursachen. Klicken Sie auf **OK**. Das Fenster **DynDNS-Account einrichten** erscheint. Überprüfen und korrigieren Sie gegebenenfalls hier die von Ihnen eingegebenen Zugangsdaten (Schritte 8 bis 11). Fahren Sie wie unter Schritt 12 beschrieben fort.

24.11.2.6 Wie Sie den Remote-Zugang ausschalten

Mit dem Wizard **Remote-Zugang** können Sie den Remote-Zugang ausschalten.

Voraussetzungen

- Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Service-Center**.

2) Klicken Sie im Navigationsbaum auf **Remote-Zugang**.

3) Klicken Sie auf **Remote-Zugang**, um den Wizard **Remote-Zugang** zu starten. Angezeigt wird, ob der Remote-Zugang über Internet oder/und ISDN eingeschaltet ist.

4) Aktivieren Sie das Optionsfeld **Remote-Zugang: aus**, um einen Remote-Zugang auszuschalten.

5) Wählen Sie aus, welche Option des Remote-Zugangs Sie ausschalten möchten:

- Wenn Sie den Remote-Zugang über Internet ausschalten möchten, aktivieren Sie das Optionsfeld **Remote-Zugang über: Internet**.
- Wenn Sie den Remote-Zugang über ISDN ausschalten möchten, aktivieren Sie das Optionsfeld **Remote-Zugang über: ISDN**.

6) Klicken Sie auf **OK & Weiter**.

7) Wenn Sie auch die zweite Option des Remote-Zugangs ausschalten wollen, klicken Sie auf **Zurück**. Wiederholen Sie die Schritte 4 bis 6.

8) Klicken Sie auf **Beenden**.

24.11.3 Online-Benutzer

Der Online-Benutzer ermöglicht die Fernsteuerung, -prüfung und -überwachung von OpenStage-Telefonen über einen Windows-PC. Das Verhalten eines OpenStage-Telefons wird über den Online-Benutzer am PC nachgebildet.

Voraussetzung für die Kommunikation mit einem OpenStage-Telefon ist, dass die Telefon-Software über einen sogenannten Dongle-Key verfügt.

Für den Zugriff auf ein OpenStage-Telefon sind folgende Eingaben über den Online-Benutzer erforderlich:

- OpenStage-Telefon-Typ
- IP-Adresse des OpenStage-Telefons
- Administrator-Passwort des OpenStage-Telefons

Informationen über die Verwendung des Online-Benutzers können folgender Dokumentation entnommen werden: *OpenStage HUSIM Phone Tester User Guide*. Der Zugriff ist möglich über das Intranet-Portal für technische Produktdokumentation `http://apps.g-dms.com:8081/techdoc/search_en.htm`.

Auch das Servicetool Manager E bietet Online-Benutzer für die Fernsteuerung, -prüfung und -überwachung von OpenStage-Telefonen.

24.11.3.1 Wie Sie Online-Benutzer starten

Voraussetzungen

- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Wartung > Online-Benutzer**. Das Anmeldefenster des Online-Benutzers wird angezeigt.

3) Wählen Sie in der Aufklappliste **Model** das Modell des gewünschten OpenStage-Telefons aus.

4) Geben Sie im Feld **Phone IP** die IP-Adresse des gewünschten OpenStage-Telefons ein.

5) Geben Sie im Feld **Password** das Administrator-Passwort des gewünschten OpenStage-Telefons ein. Standardmäßig ist das Administrator-Passwort `123456`.

6) Wählen Sie in der Aufklappliste **Protocol** das gewünschte Transportprotokoll aus.

7) Wählen Sie eine der folgenden Möglichkeiten für die Internet Protocol Version IPv:

- Wenn Sie die Internet Protocol Version 4 verwenden möchten, aktivieren Sie die Option **IPv4**.
- Wenn Sie die Internet Protocol Version 6 verwenden möchten, aktivieren Sie die Option **IPv6**.

8) Wählen Sie in der Aufklappliste **Number of Key modules** die Anzahl der Beistellgeräte aus.

9) Klicken Sie auf **OK**, um den Zugriff auf das gewünschte OpenStage-Telefon zu starten.

INFO: Informationen über die Bedienung des Online-Benutzers können Sie dem *OpenStage HUSIM Phone Tester User Guide* entnehmen, das über `http://apps.g-dms.com:8081/techdoc/search_en.htm` aufgerufen werden kann.

---

25 Migration

Beschrieben wird die technische Migration von HiPath 3000 V9 Standalone-Systemen und HiPath 3000 V9 Netzverbunden auf OpenScape Business V1.

Folgende Komunikationssysteme und Netzverbunde können migriert werden:

- HiPath 3000 V9 Standalone-System
- HiPath 3000 V9 Standalone-System mit OpenScape Office V3 HX
- HiPath 3000 V9 Netzverbund
- HiPath 3000 V9 Netzverbund mit HiPath 5000 RSM
- HiPath 3000 V9 Netzverbund mit OpenScape Office V3 LX

Die Migration von HiPath 3000 V7 und HiPath 3000 V8 auf OpenScape Business V1 ist ebenfalls möglich. In diesen Fällen muss zunächst auf HiPath 3000 V9 hochgerüstet werden und anschließend auf OpenScape Business V1.

INFO: Vor der Migration auf OpenScape Business V1 muss das HiPath 3000 V9 System einmal komplett in Betrieb genommen werden inklusive aller angeschlossenen Endgeräte.

Die Migration eines OpenScape Office V3 MX Gateways innerhalb eines HiPath 3000 V9 Netzverbunds wird zurzeit nicht unterstützt.

Ist an das HiPath 3000 V9 Kommunikationssystem zusätzlich eine OpenScape Office V3 HX angeschlossen, kann diese auf einen externen UC Booster Server hochgerüstet werden.

Die Hochrüstung eines HiPath 3000 V9 Kommunikationssystems erfolgt durch den Austausch des Mainboards, KDS-Konvertierung und anschließender Lizenzmigration.

INFO: Alle nachstehend aufgeführten Schritte zur Installation der neuen Hardware sind in der Servicedokumentation - Montage der Hardware ausführlich beschrieben.

Folgende Punkte sind vor einer Migration zu beachten:

- **Hardware-Kompatibilitätscheck**
  Bitte überprüfen Sie, ob die vorhandene Hardware weiterhin verwendet werden kann. Nicht mehr unterstützte Baugruppen oder Endgeräte müssen entfernt und ggf. durch Nachfolger ausgetauscht werden. Eine Liste finden sie hier *Nicht unterstützte Baugruppen und Endgeräte*
- **Ermittlung des Leistungsbedarfs**
  Da ein OpenScape Business Mainboard mehr Strom benötigt als ein HiPath 3000 Mainboard, ist in folgenden Fällen der Leistungsbedarf zu ermitteln (siehe Servicedokumentation, Anhang "Leistungsbedarf eines Kommunikationssystems") und falls nötig die OpenScape Business Powerbox einzusetzen:
  - bei HiPath 3000 Systemen ohne HG1500

  - bei Verwendung der UC Booster Card (OCAB)

  Bei der Migration einer HiPath 33xx/35xx nach OpenScape Business X3/X5 ist die evtl. noch genutzte Stromversorgung PSU auszutauschen gegen die aktuellere Stromversorgung UPSC-D/-DR.

- **Steckplatz-Kontrolle bei X8**

  Um eine optimale Belüftung der Basisbox zu gewährleisten, gelten für einige Baugruppen folgende Steckplatz-Einschränkungen:

  - **Analoge Teilnehmer-Baugruppen**

    Analoge Teilnehmer-Baugruppen dürfen nicht direkt rechts neben dem OCCL-Mainboard auf Steckplatz 7 gesteckt sein. In dem Steckplatz 5 links neben dem OCCL-Mainboard sollten, wenn möglich, ebenfalls keine analogen Teilnehmer-Baugruppen gesteckt sein.

  - **Stromversorgung LUNA2**

    Zwischen zwei LUNA2-Baugruppen sollte wenn möglich mindestens ein freier Steckplatz liegen.

- **Funktions-Kompatibilitätscheck**

  Bitte informieren Sie sich, welche Funktionen gegenüber HiPath 3000 V9 nicht mehr unterstützt werden oder sich geändert haben. Eine Liste finden Sie hier *Geänderte Leistungsmerkmale und Schnittstellen*.

- **Lizenzmigration**

  Bitte beachten Sie die Informationen zur Lizenzmigration, damit alle vorhandenen Leistungsmerkmale korrekt ermittelt und in das neue System übernommen werden können (siehe *Lizenzmigration*).

- **Schutzerdung**

  Für alle OpenScape Business Kommunikationssysteme ist eine Schutzerdung über einen zusätzlichen Schutzleiter zwingend erforderlich!

- **EVM-Modul**

  Das EVM-Modul wird nicht mehr benötigt. Die Funktionalität ist in Form von UC Smart (Sprachnachrichten, Ansagen, AutoAttendant) auf dem neuen Mainboard integriert. Die Sprachnachrichten und Ansagen des EVM-Moduls können nicht migriert werden.

- **HG1500**

  Die HG1500-Baugruppe wird nicht mehr benötigt. Die Funktionalität ist auf dem neuen Mainboard integriert.

  - **DSP-Kanäle**

    Bitte ermitteln Sie die Anzahl der benötigten DSP-Kanäle. DSP-Kanäle werden benötigt, um Netzübergänge von TDM-Telefonie auf VoIP zu realisieren. Bei HiPath 3000 lieferte die HG1500 und ggf. deren PDM-Module die DSP-Kanäle. OpenScape Business hat 8 DSP-Kanäle auf dem Mainboard integriert. Zur Erweiterung von DSP-Kanälen kann das DSP-Modul OCCB1 (bis zu 40 Kanäle) oder das DSP-Modul OCCB3 (bis zu 120 Kanäle) eingesetzt werden.

    Detaillierte Informationen zu DSP- und T.38-Ressourcen finden Sie im Kapitel *Systembedingte Ausbaugrenzen*.

  - **S_0-Schnittstellen**

    Alle S_0-Schnittstellen, die auf gesteckten HG 1500 Baugruppen konfiguriert sind, werden nach der KDS-Konvertierung automatisch am Slot 0 des Kommunikationssystems neu registriert.

- **Rufnummernplan im Netzverbund**
  Bei reiner Sprachvernetzung ist die offene und die geschlossene Nummerierung möglich. Bei Nutzung der UC Suite ist eine geschlossene Nummerierung im Netzverbund erforderlich (netzweite UC-Funktionalität). Bei Nutzung von UC Smart ist die offene und die geschlossene Nummerierung möglich (knotenweite UC-Funktionalität).
- **Multi-SLC**
  Sind in der HiPath 3800 mehrere SLCN-Baugruppen gesteckt, werden diese über SLC-Vernetzungsleitungen synchronisiert (Multi-SLC). Für jede SLC-Vernetzungsleitung ist ein interner S_0-Teilnehmer eingerichtet. Nach der Migration muss kontrolliert werden, dass für diese S_0-Teilnehmer das Teilnehmer-Flag **Anklopfschutz ein** deaktiviert ist.
  Ansosnten kann es zu Problemen kommen, wenn ein DECT-Telefon Roaming zu einer Basisstation durchführen möchte, die an einer anderen SLCN-Baugruppe angeschlossen ist.

25.1 Lizenzmigration

Die Lizenzmigration ist nötig für die Hochrüstung von HiPath 3000 V9 nach OpenScape Business V1. An HiPath 3000 angebundene OpenScape Office V3 LX und OpenScape Office V3 HX können ebenfalls migriert werden.

Voraussetzung für die Lizenzmigration

Folgende Voraussetzungen sind für eine erfolgreiche Lizenzmigration zu beachten:

- Es ist immer die aktuellste Version des Manager E zu verwenden.
- Eine Upgrade-Lizenz zur Hochrüstung von HiPath 3000 V9 nach OpenScape Business V1 wurde bestellt. Mit dieser Lizenz darf auch eine OpenScape Office V3 HX hochgerüstet werden, falls vorhanden.
- Für die Migration von OpenScape Office V3 LX muss eine separate Migrations-Lizenz auf OpenScape Business V1 S bestellt werden. Zusätzlich muss der Server-PC auf SLES 11 SP3 64 Bit und die neue OpenScape Business Kommunikationssoftware aktualisiert werden.
- Für die Migration von HiPath 3000 V7 oder HiPath 3000 V8 auf OpenScape Business V1 ist zuerst auf ein hochgelaufenes, mit allen Endgeräten angeschaltetes HiPath 3000 V9-System hochzurüsten, damit alle TDM-Teilnehmer übernommen werden.
- Der LAC der Upgrade-Lizenz liegt vor, um am Lizenzserver die neue Lizenz abzurufen.

Upgrade-Lizenz für HiPath 3000 / OpenScape Office V3 HX

Über die Upgrade-Lizenz werden folgende Lizenzen aus dem vorhandenen HiPath 3000 Lizenzfile in OpenScape Business Lizenzen überführt:

- IP-Teilnehmer (ComScendo)
- S_{2M}-/T1-Kanäle
- Mobility Entry (für die DISA basierte Mobility Funktion)

- Xpressions Compact Announcements, Conferencing, Mobility

Für OpenScape Office V3 HX Anschaltungen gilt:

- Pro OpenScape Office Standard User: 1x myPortal for Desktop, 1x Voicemail; 1x Fax gilt für Standard User Lizenzen in den HX Basislizenzen 5/10 und Einzellizenzen
- Pro System: 1x Company AutoAttendant, 1x Web Collaboration
- Für folgende weitere OpenScape Office HX Lizenzen wird die entsprechende Anzahl OpenScape Business Lizenzen generiert: myPortal for Outlook, myAttendant, Application Launcher, Gate View Kameras, OpenDirectory Connector, myAgent, Contact Center Fax, Contact Center e-Mail, myReports.
  Teilnehmer-Lizenzen und User-orientierte Lizenzen werden den Teilnehmern fest zugeordnet. Für myAgent und myAttendant Benutzer müssen ausreichend Lizenzen vorhanden sein.
- Im Fall einer OpenScape Office HX Voicemail Lizenz (Voicemail-Funktionalität für alle User) werden 500x OpenScape Business Voicemail-Lizenzen generiert.

Upgrade-Lizenz für OpenScape Office V3 LX

Über die Upgrade-Lizenz werden folgende Lizenzen aus der vorhandenen OpenScape Office V3 LX Lizenzdatei in OpenScape Business Lizenzen überführt:

- OpenScape Office V3 LX Basis 5/10/20 Comfort Plus User
- 1x OpenScape Business Base, 5/10/20x IP User, 5/10/20x Mobility User (max 200 pro System), 5/10/20x myPortal for Desktop, 5/10/20x Voicemail, 5/10/20x Fax, 5/10/20x Conference
- Pro System: 1x Company AutoAttendant, 1x Web Collaboration
- Pro OpenScape Office Comfort User: 1x IP User, 1x myPortal for Desktop, 1x Voicemail
- Pro OpenScape Office Comfort Plus User: 1x IP User, 1x Mobility User (max. 200 pro System), 1x myPortal for Desktop, 1x Voicemail; 1x Fax, 1x Conference
- Für folgende weitere OpenScape Office V3 LX Lizenzen wird die entsprechende Anzahl OpenScape Business Lizenzen generiert: myPortal for Outlook, myAttendant, Application Launcher, Gate View Kameras, OpenDirectory Connector, myAgent, Contact Center Fax, Contact Center e-Mail, myReports.
  Teilnehmer-Lizenzen und User-orientierte Lizenzen werden den Teilnehmern fest zugeordnet. Für myAgent und myAttendant Benutzer müssen ausreichend Lizenzen vorhanden sein.

Lizenzmigration der TDM-Teilnehmer (nur für HiPath 3000)

In OpenScape Business werden für alle TDM-Teilnehmer (UP0, a/b, S0, DECT) Teilnehmer-Lizenzen vom Typ "TDM User" benötigt. Für bereits vorhandene TDM-Teilnehmer müssen keine neuen Lizenzen gekauft werden.

Bei der Konvertierung des KDS wird automatisch die Anzahl der im HiPath 3000 System aktiven TDM-Teilnehmer ermittelt. Die benötigten TDM-User-Lizenzen

werden bei der Lizenzmigration am CLS automatisch in die neu generierte Lizenzdatei übernommen.

Die Anzahl der TDM User Lizenzen wird nach folgenden Regeln ermittelt:

- 1x TDM User Lizenz pro aktivem UP0-Port - Telefon bereit, Rufnummer verfügbar
- 1x TDM User Lizenz pro registriertem DECT-Telefon - Rufnummer verfügbar
- 1x TDM User Lizenz pro konfiguriertem a/b-Port (Rufnummer) für gesteckte Baugruppen
- 1x TDM User Lizenz pro konfiguriertem S0-Port (Rufnummer) für aktive Baugruppen

Die KDS-Konvertierung kann nur einmalig ausgeführt werden. Die Schritte für die technische Migration sind genau einzuhalten. Es ist nicht möglich, nachträglich die ermittelten Daten zu verändern.

Die Lizenzaktivierung wird offline über eine Lizenzdatei vom CLS durchgeführt. Die Beschreibung zur Durchführung der Lizenzaktivierung finden sie hier: *Lizenzaktivierung (Standalone)*.

Produkte und Funktionen ohne Lizenzmigration

Für folgende HiPath 3000 V9 und OpenScape Office V3 LX Produkte und Funktionen wird keine Lizenzmigration durchgeführt:

- OpenStage Gate View auf dem Plug-PC: OpenStage Gate View kann direkt an OpenScape Business betrieben werden.
- HG1500 B-Kanäle: Baugruppe entfällt, die Funktionalität ist auf dem neuen Mainboard integriert.
- optiClient Attendant V8: läuft nicht an OpenScape Business. Nachfolgeprodukt: OpenScape Business Attendant
- optiClient BLF V1/V2: läuft nicht an OpenScape Business. Nachfolgeprodukt: OpenScape Business BLF
- HiPath TAPI 120/170 V2: läuft nicht an OpenScape Business. Nachfolgeprodukt: OpenScape Business TAPI 120/170
- Entry VoiceMail: Modul entfällt, die Funktionalität ist auf dem neuen Mainboard integriert.
- myPortal entry Web Services Communications Clients auf dem Plug PC.
- HiPath 3000 BS4: Lizenzen für Basisstationen werden nicht mehr benötigt.
- ITSP-Amtszugang: für die Nutzung von ITSP-Kanälen für die Internet-Telefonie sind in OpenScape Business Lizenzen zu kaufen.
- Für S_0-Amt, Analog-Amt und CAS-Amt werden weiterhin keine Lizenzen benötigt.
- Für Vernetzungen und Anbindung von Fremdsystemen über Querleitungen ist pro Knoten in OpenScape Business eine Networking-Lizenz zu kaufen.

Weitere Hinweise

Bitte beachten Sie zusätzlich folgende Hinweise:

- In OpenScape Business Systemen sind alle user-orientierten Lizenzen über die Administration (WBM) den Rufnummern fest zugeordnet und damit fest an die Rufnummer gebunden. Es werden entsprechende Lizenzen benötigt.
- Das Leistungsmerkmal Deskshare User (IP-Moblity) ist in OpenScape Business lizenzpflichtig im Gegensatz zur HiPath 3000. Es müssen zusätzliche Lizenzen vom Typ "Deskshare User" gekauft werden.

Lizenzverfahren bei der Migration eines Netzverbunds

Ein bestehender HiPath 3000/5000 Netzverbund mit einer gemeinsamen Netzwerklizenzdatei ist über den CLS in Standalone-Systeme mit einzelnen Lizenzdateien aufzulösen. Jeder Knoten wird nun wie ein Standalone-System hochgerüstet und lizenziert. Bei Bedarf können die OpenScape Business Systeme am CLS wieder zu einem Netzverbund mit einer einzigen Netzwerklizenzdatei zusammengeführt werden.

OpenScape Office V3 LX mit HiPath 3000 Gateways werden wie Standalone-Systeme hochgerüstet und lizenziert. Bei Bedarf können die OpenScape Business Systeme am CLS wieder zu einem Netzverbund mit einer einzigen Netzwerklizenzdatei zusammengeführt werden.

Subscription (Linux-Software für OpenScape Business S und OpenScape Business Server)

Bei Migrationen von OpenScape Office V3 LX/HX kann bei OpenScape Business S und OpenScape Business Server eine SLES-Subscription eingerichtet werden. Der erforderliche Novell-Registrierungskey wird als LAC beim Kauf der DVD mit der OpenScape Business Kommunikationssoftware bereitgestellt.

INFO: Der bei der OpenScape Office V3 LX/HX verwendete Registrierungskey (Hosting über den Central-Update-Server) wird nicht mehr benötigt.

25.2 Migration eines HiPath 3000 V9 Standalone-Systems

Um ein HiPath 3000 V9 Standalone-System auf ein OpenScape Business Kommunikationssystem hochzurüsten, sind die nachstehend beschriebenen Migrationsschritte durchzuführen.

WICHTIG: Bei der Erstinbetriebnahme von OpenScape Business ist der Ladezustand des Akkus auf dem neuen OpenScape Business Mainboard nicht definiert. Um einen ausreichenden Ladezustand zu erreichen, muss das System mindestens 2 Tage am Stromnetz bleiben. Wird das System vom Stromnetz getrennt, kann es bei unzureichendem Ladezustand des Akkus vorkommen, dass die Activation Period wegen Zeitmanipulation gesperrt wird und die für die Lizenzierung notwendige XML-Datei nicht mehr zur Verfügung steht.

Führen Sie folgende Migrationschritte der Reihe nach durch:

1. **HiPath 3000 V9 KDS aus dem System laden**
   Laden Sie mit Hilfe der neuesten Manager E Version den aktuellen HiPath 3000 V9 KDS aus dem HiPath 3000 V9 System.
2. **HG1500 Einstellungen notieren (optional)**
   Sind eine oder mehrere HG1500 Baugruppen gesteckt, müssen Sie sich die HG1500-Einstellungen, die in Bezug auf die Standard-Einstellungen geändert wurden, mit Hilfe des HG1500-WBM notieren:
   - IP-Routing
   - PSTN-Routing
   - IP-Firewall
   - MAC-Firewall
   - Application Firewall
   - IP-Accounting
   - IP-Mapping
   - SNMP
3. **HiPath 3000 V9 KDS konvertieren**
   Konvertieren Sie mit Hilfe der neuesten Manager E Version den aktuellen HiPath 3000 V9 KDS in den OpenScape Business KDS.
4. **Hardware austauschen**
   Tauschen Sie das HiPath 3000 Mainboard gegen das neue OpenScape Business Mainboard aus. Entfernen Sie auch alle HG1500 Baugruppen und alle nicht mehr unterstützten Baugruppen und Submodule. Alle OpenScape Business Kommunikationssysteme sind mit einem zusätzlichen Schutzleiter zu erden.
5. **Erstinstallation durchführen**
   Konfigurieren Sie das Kommunikationssystem über das WBM mit dem Wizard **Erstinstallation**. Berücksichtigen Sie dabei auch die HG1500 Einstellungen, die Sie sich vorher notiert haben.
6. **Konvertierten KDS laden**
   Laden Sie den konvertierten KDS mit Hilfe der neuesten Manager E Version in das OpenScape Business System. Anschließend startet das OpenScape Business System automatisch neu.
7. **Neue Lizenzdatei am CLS generieren**
   Generieren Sie am CLS eine neue Lizenzdatei mit dem LAC der Upgrade-Lizenz, der Konfigurationsdatei (XML-Datei) und der Locking-ID von OpenScape Business.
8. **Lizenzen aktivieren und zuordnen**
   Lizenzieren Sie das OpenScape Business Kommunikationssystem innerhalb von 30 Tagen mit Hilfe der Lizenzdatei.
9. **LCR-Einträge zurücksetzen**
   Bei Bedarf können Sie die im HiPath 3000 System konfigurierten LCR-Einträge (wie z. B. Wahlpläne, Wegetabellen, Wahlregeln) auf die Standard-Einträge von OpenScape Business zurücksetzen. Diese Einstellung finden Sie im WBM im Wizard **Basisinstallation**.

25.2.1 Wie Sie den KDS aus HiPath 3000 V9 laden

Voraussetzungen

- Ein HiPath 3000 Kommunikationssystem (HiPath 3300, HiPath 3350, HiPath 3500, HiPath 3550 oder HiPath 3800) ist in der Version 9 vorhanden.
- Alle Telefone sind angeschlossen und aktiv.
- Der neueste Manager E ist auf dem Admin-PC installiert.
- Der Admin-PC ist mit dem HiPath 3000 Kommunikationssystem verbunden.

Schritt für Schritt

1) Melden Sie sich auf dem Admin-PC am Manager E an.

2) Klicken Sie in der Menüleiste auf **Datei > Übertragen**.

3) Klicken Sie auf die Registerkarte **Kommunikation**.

4) Aktivieren Sie im Bereich **Zugang** die entsprechende Option, je nach Verbindungsart des Admin-PC zum System.

5) Aktivieren Sie das Optionsfeld **KDS lesen/schreiben** und klicken Sie auf **Anlage -> PC**.

6) Klicken Sie auf **OK**. Der KDS wird von HiPath 3000 V9 zum Manager E übertragen.

7) Klicken Sie nach erfolgreicher Übertragung auf **OK** und anschließend auf **Schließen**.

8) Klicken Sie in der Menüleiste auf **Datei > KDS speichern unter** und speichern Sie den KDS auf dem Admin-PC in einem Verzeichnis Ihrer Wahl.

Nächste Schritte

Wie Sie die HG1500 Einstellungen auslesen

25.2.2 Wie Sie die HG1500 Einstellungen auslesen

Voraussetzungen

- Eine oder mehrere HG1500 Baugruppen sind gesteckt.
- Sie sind am Manager E angemeldet.

Schritt für Schritt

1) Klicken Sie im Manager E in der Anlagenansicht auf den Eintrag der HG1500. Das WBM der HG1500 öffnet sich.

2) Notieren Sie sich die Einstellungen, die gegenüber den Standard-Einstellungen geändert wurden. Die HG1500 Einstellungen werden bei der Konvertierung des KDS nicht übernommen und müssen bei der Erstinbetriebnahme der OpenScape Business im WBM nochmals konfiguriert werden.

Nächste Schritte

Wie Sie den HiPath 3000 V9 KDS konvertieren

25.2.3 Wie Sie den HiPath 3000 V9 KDS konvertieren

Voraussetzungen

- Ein HiPath 3000 Kommunikationssystem (HiPath 3300, HiPath 3350, HiPath 3500, HiPath 3550 oder HiPath 3800) ist in der Version 9 vorhanden.
- Der Admin-PC ist mit dem HiPath 3000 Kommunikationssystem verbunden.

Schritt für Schritt

1) Klicken Sie in der Menüleiste auf **Datei > KDS konvertieren**.

2) Wählen Sie den zuvor auf dem Admin-PC abgespeicherten KDS aus und klicken Sie auf **OK**.

3) Geben Sie als Kundendaten Ihren **Namen** und Ihre **Vertragsnummer** ein und klicken Sie auf **Weiter**.

4) Wählen Sie als **Version** den Eintrag **OpenScape Business V1** aus und klicken Sie auf **Weiter**.

5) Bestätigen Sie die Hinweise auf nicht mehr unterstützte Baugruppen mit **OK**.

6) Bestätigen Sie die Anzeige der gesteckten Baugruppen mit **Weiter**.

7) Klicken Sie in der Menüleiste auf **Datei > KDS speichern unter** und speichern Sie den KDS unter einem anderen Namen auf dem Admin-PC in einem Verzeichnis Ihrer Wahl.

8) Schließen Sie den Manager E.

Nächste Schritte

Wie Sie die Hardware bei HiPath 3300/3500 austauschen oder

Wie Sie die Hardware bei HiPath 3350/3550 austauschen oder

Wie Sie die Hardware bei HiPath 3800 austauschen

25.2.4 Wie Sie die Hardware bei HiPath 3300/3500 austauschen

Voraussetzungen

- Laufendes HiPath 3000 Kommunikationssystem für den Rackbetrieb (HiPath 3300 oder HiPath 3500) in Version 9.
- OpenScape Business Mainboard OCCMR.



WARNUNG

Elektrischer Schlag durch Berühren spannungsführender Leitungen

Stellen Sie sicher, dass für das Kommunikationssystem ein zusätzlicher Schutzleiter mit dem geforderten Mindest-Leiterquerschnitt vorhanden ist (siehe Servicedokumentation, Montage der Hardware).

Schritt für Schritt

1) Schalten Sie die HiPath 3000 aus und ziehen Sie anschließend den Netzstecker.

2) Entfernen Sie alle Stecker vom Mainboard, wie z. B. analoge Teilnehmer, ISDN-Leitungen, usw.

3) Lösen Sie die beiden Feststellschrauben in der Frontblende des Mainboards.

4) Lösen Sie mit zwei Baugruppenschlüssel (C39165-A7027-C26) das Mainboard von der Backplane.

5) Ziehen Sie vorsichtig mit beiden Händen das HiPath 3000 Mainboard waagrecht aus dem Baugruppenrahmen und legen Sie es auf einer flachen, geerdeten und leitfähigen Unterlage ab.

6) Entfernen Sie evtl. vorhandene HG1500 Baugruppen aus dem Gehäuse. Die frei gewordenen HG1500-Steckplätze können für zusätzliche Baugruppen verwendet werden.

7) Ziehen Sie falls vorhanden alle nicht mehr unterstützten Baugruppen aus dem Gehäuse. Die frei gewordenen Steckplätze können für zusätzliche Baugruppen verwendet werden.

8) Entfernen Sie alle auf dem HiPath 3000 Mainboard gesteckten Submodule und stecken Sie diese (falls noch benötigt und unterstützt) auf das OpenScape Business Mainboard.

9) Entfernen Sie die Akku-Schutzfolie auf dem neuen OpenScape Business Mainboard OCCMR.

10) Schieben Sie vorsichtig mit beiden Händen das OpenScape Business Mainboard OCCMR waagerecht in den Steckplatz des Baugruppenrahmens, wo vorher das HiPath 3000 Mainboard steckte.

11) Stecken Sie wieder alle Stecker in das Mainboard, wie z. B. analoge Teilnehmer, ISDN-Leitungen, usw.

INFO: Bei Verwendung von mehr als 2 analogen a/b-Ports in HiPath 3300 oder 3500 sind in OpenScape Business 1 bzw. 2 Y-Adapterkabel erforderlich. Es müssen bis zu 4 a/b-Ports über die 2 physikalischen RJ11-Buchsen herausgeführt werden. Das neue Mainboard hat aus Platzgründen lediglich 2 RJ11-Buchsen, über die 4 a/b-Teilnehmer anzubinden sind.

12) Stecken Sie, falls noch nicht geschehen, die SDHC-Karte in den SDHC-Kartenslot des Mainboards, bis sie einrastet. Die Metallkontakte der SDHC-Karte müssen dabei Richtung Mainboard zeigen.

> ***INFO:*** Vergewissern Sie sich, dass der Schreibschutz der SDHC-Karte deaktiviert ist (Schalter Richtung Metallkontakte).

13) Verbinden Sie Ihr Kommunikationssystem ordnungsgemäß mit dem Schutzleiter.

14) Stecken Sie den Netzstecker wieder ein und fahren Sie das System hoch.

Nächste Schritte

Wie Sie die Erstinstallation durchführen

25.2.5 Wie Sie die Hardware bei HiPath 3350/3550 austauschen

Prerequisites

- Laufendes HiPath 3000 Kommunikationssystem für den Wandbetrieb (HiPath 3350 oder HiPath 3550) in Version 9.
- OpenScape Business Mainboard OCCM.



WARNUNG

Elektrischer Schlag durch Berühren spannungsführender Leitungen

Stellen Sie sicher, dass für das Kommunikationssystem ein zusätzlicher Schutzleiter mit dem geforderten Mindest-Leiterquerschnitt vorhanden ist (siehe Servicedokumentation, Montage der Hardware).

Step by Step

1) Schalten Sie die HiPath 3000 aus und ziehen Sie anschließend den Netzstecker.

2) Lösen Sie die Verriegelung des Gehäuses und entfernen Sie das Gehäuse.

3) Entfernen Sie die Abdeckung.

4) Entfernen Sie alle Steckverbinder (Edge-Connectoren) vom Mainboard, wie z. B. analoge Teilnehmer, ISDN-Leitungen, usw.

5) Entfernen Sie den Baugruppenriegel.

6) Entfernen Sie vorsichtig das HiPath Mainboard aus dem Baugruppenrahmen und legen Sie es auf einer flachen, geerdeten und leitfähigen Unterlage ab.

7) Entfernen Sie evtl. vorhandene HG1500 Baugruppen aus dem Gehäuse. Die frei gewordenen HG1500-Steckplätze können für zusätzliche Baugruppen verwendet werden.

8) Ziehen Sie falls vorhanden alle nicht mehr unterstützten Baugruppen aus dem Gehäuse. Die frei gewordenen Steckplätze können für zusätzliche Baugruppen verwendet werden.

9) Entfernen Sie alle auf dem HiPath 3000 Mainboard gesteckten Submodule und stecken Sie diese (falls noch benötigt und unterstützt) auf das OpenScape Business Mainboard.

10) Entfernen Sie die Akku-Schutzfolie auf dem neuen OpenScape Business Mainboard OCCM.

11) Stecken Sie vorsichtig das OpenScape Business Mainboard OCCM in den gleichen Slot, wo vorher das HiPath 3000 Mainboard steckte.

12) Stecken Sie wieder alle Steckverbinder (Edge-Connectoren) in das Mainboard, wie z. B. analoge Teilnehmer, ISDN-Leitungen, usw. Beachten Sie, dass die Stecker für die ISDN-Leitungen zuerst durch das Loch des neuen Baugruppenriegels geführt werden müssen.

13) Stecken Sie, falls noch nicht geschehen, die SDHC-Karte in den SDHC-Kartenslot des Mainboards, bis sie einrastet. Die Metallkontakte der SDHC-Karte müssen dabei Richtung Mainboard zeigen.

> ***INFO:*** Vergewissern Sie sich, dass der Schreibschutz der SDHC-Karte deaktiviert ist (Schalter Richtung Metallkontakte).

14) Bringen Sie den neuen Baugruppenriegel an.

15) Verbinden Sie Ihr Kommunikationssystem ordnungsgemäß mit dem Schutzleiter.

16) Setzen Sie das Gehäuse auf und verriegeln Sie es.

17) Stecken Sie den Netzstecker wieder ein und fahren Sie das System hoch.

Next steps

Wie Sie die Erstinstallation durchführen

25.2.6 Wie Sie die Hardware bei HiPath 3800 austauschen

Voraussetzungen

- Laufendes HiPath 3800 Kommunikationssystem in Version 9.
- OpenScape Business Mainboard OCCL.



WARNUNG

Elektrischer Schlag durch Berühren spannungsführender Leitungen

Stellen Sie sicher, dass für das Kommunikationssystem ein zusätzlicher Schutzleiter mit dem geforderten Mindest-Leiterquerschnitt vorhanden ist (siehe Servicedokumentation, Montage der Hardware).

Schritt für Schritt

1) Schalten Sie die HiPath 3000 aus und ziehen Sie anschließend den Netzstecker.

2) Entfernen Sie alle Stecker vom Mainboard.

3) Ziehen Sie vorsichtig das HiPath 3000 Mainboard aus dem Baugruppenrahmen und legen Sie es auf einer flachen, geerdeten und leitfähigen Unterlage ab.

4) Ziehen Sie evtl. vorhandene HG1500 Baugruppen aus dem aus dem Baugruppenrahmen. Die frei gewordenen HG1500-Steckplätze können für zusätzliche Baugruppen verwendet werden.

5) Ziehen Sie falls vorhanden alle nicht mehr unterstützten Baugruppen aus dem aus dem Baugruppenrahmen. Die frei gewordenen Steckplätze können für zusätzliche Baugruppen verwendet werden.

6) Entfernen Sie alle auf dem HiPath 3000 Mainboard gesteckten Submodule und stecken Sie diese (falls noch benötigt und unterstützt) auf das OpenScape Business Mainboard.

7) Entfernen Sie die Akku-Schutzfolie auf dem neuen OpenScape Business Mainboard OCCL.

8) Stecken Sie vorsichtig das OpenScape Business Mainboard OCCL in den gleichen Slot, wo vorher das HiPath 3000 Mainboard steckte.

9) Stecken Sie wieder alle Stecker in das Mainboard.

10) Stecken Sie, falls noch nicht geschehen, die SDHC-Karte in den SDHC-Kartenslot des Mainboards, bis sie einrastet. Die Metallkontakte der SDHC-Karte müssen dabei Richtung Mainboard zeigen.

> ***INFO:*** Vergewissern Sie sich, dass der Schreibschutz der SDHC-Karte deaktiviert ist (Schalter Richtung Metallkontakte).

11) Verbinden Sie Ihr Kommunikationssystem ordnungsgemäß mit dem Schutzleiter.

12) Stecken Sie den Netzstecker wieder ein und fahren Sie das System hoch.

Nächste Schritte

Wie Sie die Erstinstallation durchführen

25.2.7 Wie Sie die Erstinstallation durchführen

Die Erstinstallation des Kommunikationssystems ist im Kapitel "Erstinstallation OpenScape Business X" im Unterkapitel "Integration ins Kunden-LAN" beschrieben (siehe *Integration ins Kunden-LAN*).

Die Erstinstallation umfasst die Konfiguration der IP-Adresse des Systems, die DHCP-Einstellungen sowie Länder- und Zeiteinstellungen.

Hatte das HiPath 3000 System zusätzlich eine HG 1500 installiert, so sollte bei der Erstinstallation für die IP-Adresse des OpenScape Business Systems die IP-Adresse der HG 1500 verwendet werden.

Nach erfolgreicher Erstinstallation führt das Kommunikationssystem einen Neustart durch.

Nächste Schritte

Wie Sie den konvertierten KDS in das neue System laden

25.2.8 Wie Sie den konvertierten KDS in das neue System laden

Voraussetzungen

- Die Hardware wurde ausgetauscht.
- Der Admin-PC ist mit dem OpenScape Business Kommunikationssystem verbunden (über die LAN-Schnittstelle).
- Der Admin-PC ist so konfiguriert, dass er IP-Adresse und Netzmaske vom DHCP-Server von OpenScape Business empfangen kann.

Schritt für Schritt

1) Melden Sie sich auf dem Admin-PC am Manager E an.

2) Klicken Sie in der Menüleiste auf **Datei > KDS öffnen**.

3) Navigieren Sie zum Ablageort des konvertierten OpenScape Business KDS und klicken Sie auf **OK**.

4) Bestätigen Sie den Hinweis mit **OK**.

5) Klicken Sie in der Menüleiste auf **Datei > Übertragen**.

6) Klicken Sie auf die Registerkarte **Kommunikation**.

7) Aktivieren Sie im Bereich **Zugang** die Option **IP - HiPath** und geben Sie im Feld IP-Adresse die IP-Adresse des OpenScape Business Kommunikationssystem sein, Standard: `192.168.1.2`.

8) Aktivieren das Optionsfeld **Sicherheit**.

9) Klicken Sie auf Kennwort ändern.

10) Geben Sie altes und neues Kennwort ein und bestätigen Sie mit **OK**.

11) Aktivieren Sie das Optionsfeld **KDS lesen/schreiben**.

12) Aktivieren Sie die Kontrollkästchen **Gebühren** und **Hardware** und klicken Sie auf **PC -> Anlage**.

13) Klicken Sie auf **OK**. Der KDS wird vom Manager E zum System übertragen.

14) Klicken Sie nach erfolgreicher Übertragung des KDS auf **OK** und anschließend auf **Schließen**.

15) Beenden Sie den Manager E. Das System führt automatisch einen Neustart durch!

Nächste Schritte

Wie Sie eine neue Lizenzdatei generieren

25.2.9 Wie Sie eine neue Lizenzdatei generieren

Voraussetzungen

- Der LAC der Upgrade-Lizenz ist vorhanden.
- Die Registrierungsdaten des Kunden liegen vor.

Schritt für Schritt

1) Melden Sie sich am WBM mit dem Profil **Advanced** an.

2) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.

3) Notieren Sie sich die Locking ID von OpenScape Business, die oberhalb der Tabelle angezeigt wird.

4) Klicken Sie im Navigationsbaum auf **Registrierung**.

5) Geben Sie Ihre Daten ein und klicken Sie auf **OK & Weiter**.

6) Klicken Sie auf **Daten exportieren**. Es wird eine Konfigurationsdatei (XML-Datei) generiert mit den Registrierungsdaten und den Inventory-Informationen inklusive der Anzahl der angeschlossenen TDM-Teilnehmer.

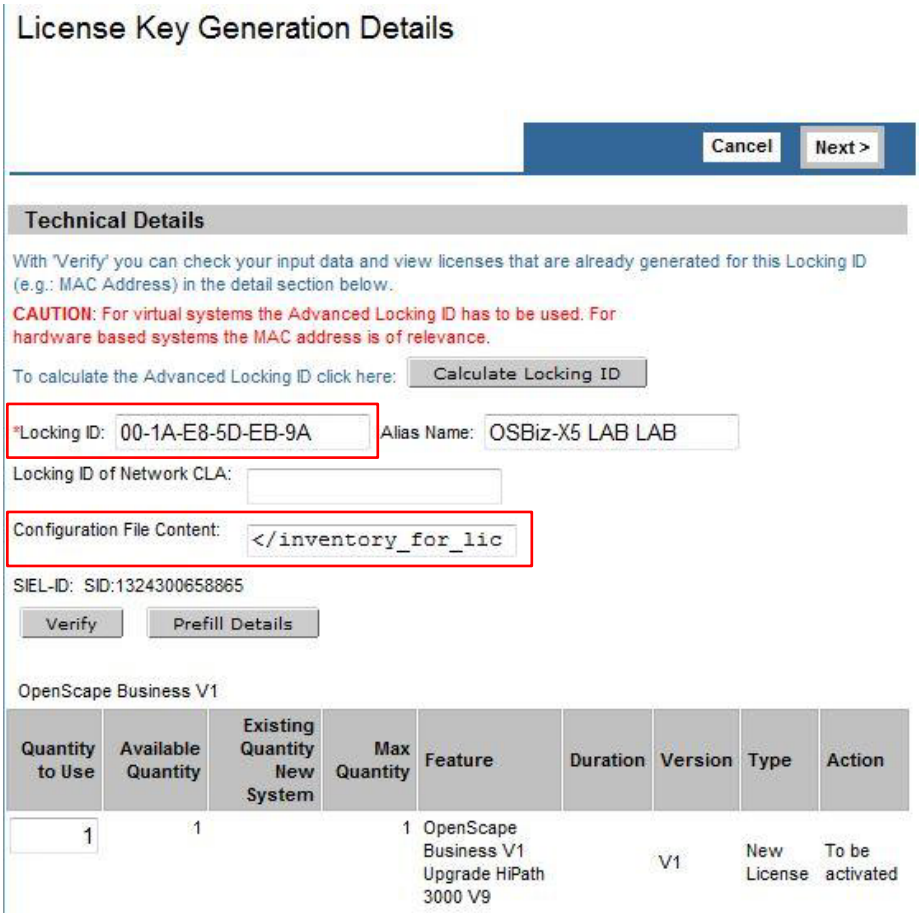
7) Speichern Sie die Konfigurationsdatei in einem Verzeichnis Ihrer Wahl.

8) Melden Sie sich am CLS mit Benutzernamen und Kennwort an.

9) Klicken Sie im Menübaum auf **License > Generate License Key**.

10) Geben Sie unter **LAC** den LAC der Upgrade-Lizenz ein und klicken sie auf **Generate Key**.

11) Markieren Sie das Leistungsmerkmal **OpenScape Business V1 Update HiPath 3000 V9** und klicken sie erneut auf **Generate Key**.



12) Geben Sie im Feld **Locking ID** die Locking ID von OpenScape Business ein.

13) Öffnen Sie die Konfigurationsdatei mit einem Text-Editor (z. B. Notepad) und kopieren Sie den kompletten Inhalt aus der Konfigurationsdatei in das Feld **Configuration File Content**.

14) Klicken Sie auf **Next** und folgen Sie den Anweisungen, um eine neue Lizenzdatei zu generieren.

> ***INFO:*** Die Prozedur der Lizenzmigration am CLS ist nur einmal möglich. Achten Sie daher bitte auf korrekte Angaben!

15) Speichern Sie die neue Lizenzdatei in einem Verzeichnis Ihrer Wahl.

Nächste Schritte

Wie Sie die Lizenzdatei offline aktivieren

25.2.10 Wie Sie die Lizenzdatei offline aktivieren

Die Offline-Lizenzaktivierung ist im Kapitel "Lizenzierung" im Unterkapitel "Lizenzaktivierung (Standalone)" beschrieben (*Wie Sie Lizenzen offline aktivieren (Standalone)*).

Nächste Schritte

Wie Sie Lizenzen zuordnen

25.2.11 Wie Sie Lizenzen zuordnen

Die Lizenzzuordnung ist im Kapitel "Lizenzierung" im Unterkapitel "Lizenzzuordnung (Standalone)" beschrieben (*Lizenzzuordnung (Standalone)*).

25.2.12 Wie Sie die LCR-Einträge zurücksetzen

Die Basisinstallation des Kommunikationssystems ist im Kapitel "Erstinstallation OpenScape Business X" im Unterkapitel "Basiskonfiguration" beschrieben (siehe *Basiskonfiguration*).

Die Basisinstallation umfasst die Konfiguration der Systemrufnummer, der Teilnehmer sowie den Zugang zum Internet und die Internet-Telefonie.

Im Wizard **Basisinstallation** finden Sie im Fenster **Zentrale Teilnehmer-Funktionen** ein zusätzliches Optionsfeld ***!Delete the configured LCR data and initialize the LCR with the OSBiz default data**. Dieses Optionsfeld erscheint nur, wenn zuvor ein konvertierter KDS in das System geladen wurde. Wird dieses Optionsfeld aktiviert, werden die im HiPath 3000 System konfigurierten LCR-Einträge gelöscht und durch die Standard-Einträge des OpenScape Business Systems ersetzt.

25.3 Migration eines HiPath 3000 V9 Standalone-Systems mit OpenScape Office V3 HX

Um ein HiPath 3000 V9 Standalone-System mit angeschlossener OpenScape Office V3 HX auf ein OpenScape Business Kommunikationssystem mit UC Booster hochzurüsten, sind die nachstehend beschriebenen Migrationsschritte durchzuführen.

Die UC-Funktionalität einer OpenScape Office V3 HX wird auf den externen OpenScape Business V1 UC Booster Server abgebildet.

Voraussetzung für die Migration ist ein HiPath 3000 V9 System ab V9 R2.7.0 mit einer OpenScape Office V3 HX ab V3 R3FR6. Ältere HiPath 3000 V9 und OpenScape Office V3 HX Versionen müssen vor der Migration auf diesen Stand

hochgerüstet werden. Für den OpenScape Business UC Booster Server muss zuerst auf die OpenScape Business Software V1 R2.2.1331 (Version 1, Minor Release 2, FixRelease 2) hochgerüstet werden. Nach erfolgreicher Migration kann auf die neueste Version aktualisiert werden.

Folgende UC-Konfigurations- und Benutzerdaten werden übernommen:

- Ansagen
- Bilder
- Sprachnachrichten
- Faxe
- Journal
- Contact Center Daten
- Benutzerkonfiguration
- Benutzer-Profile
- Externes Verzeichnis
- Zeitpläne

Folgende UC-Konfigurations- und Benutzerdaten werden **nicht** übernommen und müssen im UC Booster Server neu konfiguriert werden:

- Web-Services (z. B. XMpp, Web Collaboration, Mobility)
- Open Directory Service
- OpenStage Gate View

Migrationsschritte

Führen Sie folgende Schritte der Reihe nach durch:

1. **Agenten-IDs notieren** (nur bei Nutzung des Contact Centers)
   Notieren Sie sich die Zuordnung der Agenten-IDs zu den Teilnehmern der UC Suite, da diese Zuordnung nicht migriert wird. Die Zuordnung muss mit dem Wizard **Anrufverteilung** im WBM des OpenScape Business Kommunikationssystems neu konfiguriert werden.
2. **OpenScape Office V3 HX Backup-Set erstellen**
   Erstellen Sie über das WBM von OpenScape Office V3 HX ein Backup-Set auf ein externes Medium.
   Genauere Informationen finden Sie in der Online-Hilfe des OpenScape Office Assistant.
3. **HiPath 3000 V9 hochrüsten**
   Führen Sie die Hochrüstung von HiPath 3000 V9 nach OpenScape Business V1 wie bei der Migrationsbeschreibung eines Standalone-Systems durch. Die Lizenzen der OpenScape Office V3 HX werden bei der Lizenzmigration am Lizenzserver nach OpenScape Business übernommen. Die Lizenzdatei enthält sowohl Lizenzdaten der OpenScape Business X3/X5/X8 als auch der UC-Suite.
4. **UC Booster Server ins Kunden-LAN integrieren**
   Auf dem neuen Server-PC (Linux-Server) wird das Linux-Betriebssystem SLES 11 SP3 64 Bit installiert und anschließend die Kommunikationssoftware. Details finden Sie in der *Installationsanleitung OpenScape Business V1, Linux-Server*.

5. **UC Booster aktivieren**
   Aktivieren Sie die UC Booster Funktionalität im WBM des OpenScape Business Kommunikationssystems (Grundinstallation - Erstinstallation - Paket mit UC Suite auf OSBiz UC Booster-Server) und tragen Sie die IP-Adresse des neuen Server-PCs ein (wenn möglich die gleiche IP-Adresse wie die des alten Server-PCs). Stellen Sie sicher, dass die UC Suite auf dem UC Booster Server aktiv ist.
   Genauere Informationen finden Sie im Kapitel "Erstinstallation OpenScape Business X3/X5/X8" unter *Wie Sie die UC-Lösung festlegen*.
6. **UC Booster konfigurieren**
   Im WBM des UC Booster Servers muss die IP-Adresse des Kommunikationssystems angegeben werden.
   Genauere Informationen finden Sie im Kapitel "Erstinstallation OpenScape Business UC Booster" unter *IP-Adresse des Kommunikationssystems bekannt geben*.
7. **OpenScape Office V3 HX Backup-Set konvertieren**
   Das auf dem externen Medium gesicherte OpenScape Office V3 HX Backup-Set muss über ein Linux-Script in ein OpenScape Business V1 Backup-Set konvertiert werden. Dafür benötigen Sie Linux-Kenntnisse. Anschließend ist das konvertierte Backup-Set über das WBM in den UC Booster Server zu laden. Danach stehen die o.g. UC-Konfigurations- und Benutzerdaten zur Verfügung.
   Genauere Informationen finden Sie in diesem Kapitel unter *Wie Sie ein OpenScape Office V3 HX Backup-Set konvertieren*.
8. **OpenScape Office V3 HX aktualisieren**
   Aktualisieren Sie OpenScape Office V3 HX auf den neuesten Softwarestand.

25.3.1 Wie Sie ein OpenScape Office V3 HX Backup-Set konvertieren

Voraussetzungen

- Der OpenScape Business UC Booster Server ist betriebsbereit.
- Das OpenScape Office V3 HX Backup-Set liegt auf dem externen Medium vor.

Schritt für Schritt

1) Kopieren Sie das OpenScape Office V3 HX Backup-Set von dem externen Medium auf den Server-PC (Linux-Server) in folgendes Verzeichnis:

```
/mnt/persistent/apollo/
```

2) Öffnen sie ein Terminal auf dem Server-PC oder verbinden sie sich mit einer SSH-Shell mit dem Server-PC. Sie benötigen root-Rechte.

3) Wechseln Sie zum Backup-Verzeichnis mit folgendem Kommando:

```
cd /mnt/persistent/backup/
```

4) Rufen Sie das Konvertierungsscript auf wie folgt:

```
/opt/symappl/services/backup/script/migrate.sh /mnt/
persistent/apollo/<Name des Backup-Sets>
```

Beispiel:

```
/opt/symappl/services/backup/script/migrate.sh /mnt/
persistent/apollo/BackupSet_130913-0400007.tar
```

5) Nachdem das Konvertierungsscript durchlaufen ist, kann das konvertierte Backup-Set für den Restore verwendet werden.

25.4 Migration eines HiPath 3000 V9 Systems auf OpenScape Business UC Booster

Um ein HiPath 3000 V9 Kommunikationssystem auf ein OpenScape Business Kommunikationssystem mit UC Booster Funktionalität hochzurüsten, sind die nachstehend beschriebenen Migrationsschritte durchzuführen.

Für die UC Booster Funktionalität wird je nach Anzahl der UC Benutzer eine UC Booster Card oder ein externer UC Booster Server verwendet.

Migrationsschritte

Führen Sie folgende Schritte der Reihe nach durch:

1. **HiPath 3000 V9 hochrüsten**
   Führen Sie die Hochrüstung von HiPath 3000 V9 nach OpenScape Business V1 wie bei der Migrationsbeschreibung eines Standalone-Systems durch.
2. **Alternative 1: UC Booster Card ins Gehäuse von OpenScape Business stecken**
   Falls Sie die UC Booster Card bevorzugen, wird diese Karte während der Hochrüstung von HiPath 3000 V9 ins Gehäuse gesteckt.
   Details finden Sie in der *Servicedokumentation, Montage der Hardware, Kapitel "Baugruppen - Beschreibung der Baugruppen - OCAB"*.
3. **Alternative 2: UC Booster Server ins Kunden-LAN integrieren**
   Falls Sie den externen UC Booster Server bevorzugen, wird auf einem Server-PC das Linux-Betriebssystem SLES 11 SP3 64 Bit installiert und anschließend die Kommunikationssoftware. Details finden Sie in der *Installationsanleitung OpenScape Business V1, Linux-Server*.
4. **UC Booster manuell aktivieren**
   Die automatische Aktivierung der UC Booster Funktionalität ist bei einer Migration nicht möglich. Daher muss die UC Booster Funktionalität manuell im WBM aktiviert werden.
   Genauere Informationen finden Sie unter *Wie Sie UC Booster manuell aktivieren*.
5. **UC Booster konfigurieren**
   Die UC Booster Funktionalität wird im WBM konfiguriert.

25.4.1 Wie Sie UC Booster manuell aktivieren

Voraussetzungen

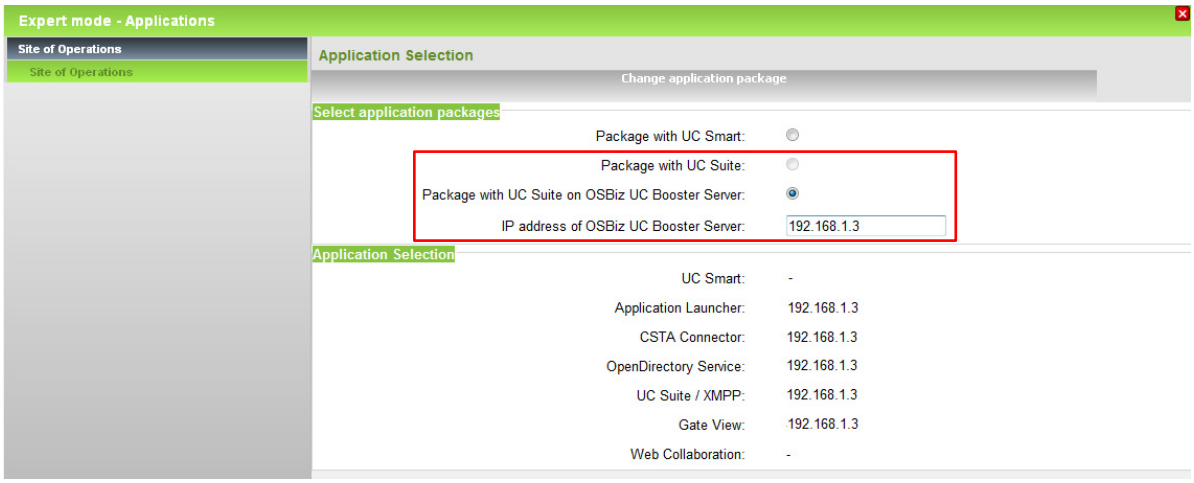
- Sie sind am WBM mit dem Profil **Expert** angemeldet.

Schritt für Schritt

1) Klicken Sie in der Navigationsleiste auf **Experten-Modus**.

2) Klicken Sie im Navigationsbaum auf **Applikationen > Applikationsauswahl**.

3) Klicken Sie im Menübaum auf **Applikations Auswahl > Applikations Auswahl**.



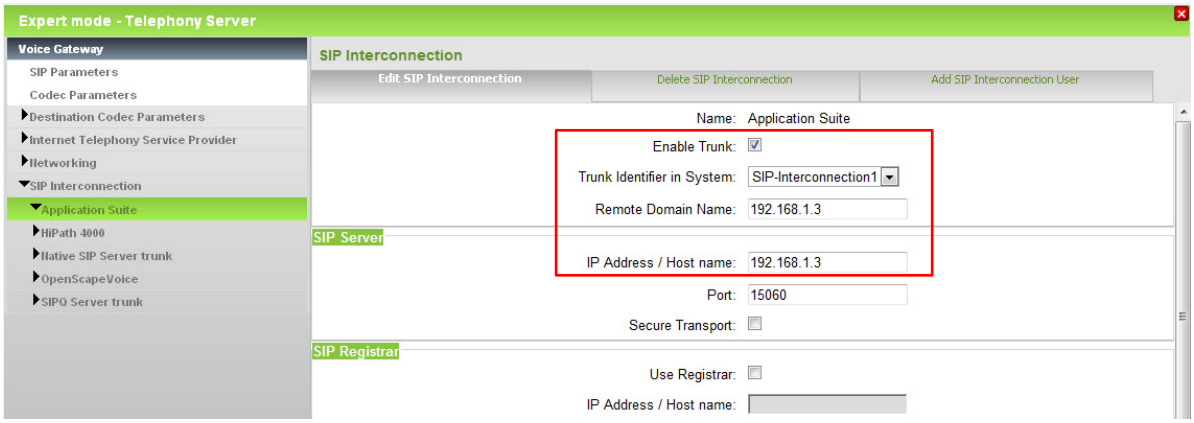
4) Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie die UC Booster Funktionalität mit der UC Booster Card nutzen möchten, klicken Sie auf **Paket mit UC Suite**.
- Wenn Sie die UC Booster Funktionalität mit dem UC Booster Server nutzen möchten, klicken Sie auf **Paket mit UC Suite auf OSBiz UC Booster-Server** und geben Sie zusätzlich im Feld **IP-Adresse des OSBiz UC Booster-Servers** die IP-Adresse des externen Linux-Servers an.

5) Klicken Sie auf **Übernehmen**.

6) Klicken Sie im Navigationsbaum auf **Telephonie > Sprachgateway**.

7) Klicken Sie im Menübaum auf **Sprachgateway > SIPQ-Verbindung > Application Suite**.



8) Aktivieren Sie das Kontrollkästchen **Trunk aktivieren**.

9) Wählen Sie in der Aufklappliste **Trunk-ID im System** den Eintrag **SIPQ-Verbindung 1**.

10) Geben Sie in den Felder **Name der Remote-Domäne** und **IP Adresse/Host-Name** die IP-Adresse der UC Booster Card oder des UC Booster Servers ein, z. B. `192.168.1.3`.

11) Klicken Sie auf **Übernehmen**.

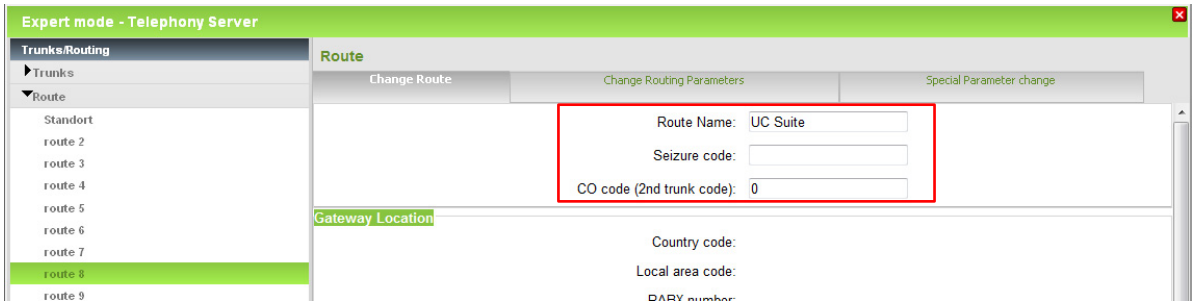
12) Klicken Sie im Menübaum auf **SIPQ-Verbindungsteilnehmer**.

13) Geben Sie unter **Benutzer-ID** den Namen `Application_Suite-User` ein. Lassen Sie die Felder **Autorisierungsname**, **Kennwort** und **Kennwort wiederholen** leer.

14) Klicken Sie auf **Übernehmen**.

15) Klicken Sie im Navigationsbaum auf **Telephonie > Leitungen/Vernetzung**.

16) Klicken Sie im Menübaum auf **Leitungen/Vernetzung > Richtung > Rtg. 8**.



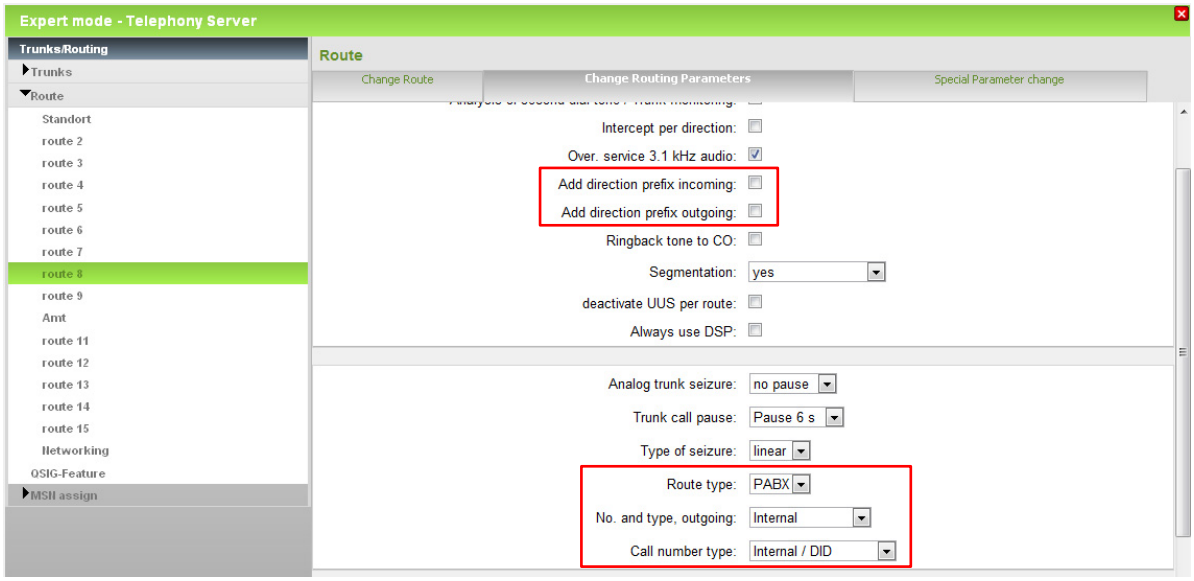
17) Geben Sie für die Richtung 8 in der Registerkarte **Richtung ändern** im Feld **Richtungsname** den Namen `UC Suite` ein.

18) Vergewissern Sie sich, dass das Feld **Richtungskennzahlen** leer ist.

19) Geben Sie im Feld **Amtskennziffer (2. AKZ)** den Wert `0` ein.

20) Klicken Sie auf **Übernehmen**.

21) Klicken Sie auf die Registerkarte **Richtungsparameter ändern**.



22) Deaktivieren Sie die Kontrollkästchen **Rtg.-Präfix ergänzen kommend** und **Rtg.-Präfix ergänzen gehend**.l

23) Wählen Sie in der Aufklappliste **Richtungsart** den Eintrag **PABX**.

24) Wählen Sie in der Aufklappliste **Nr-Typ, gehend** den Eintrag **Intern**.

25) Wählen Sie in der Aufklappliste **Rufnummer Typ** den Eintrag **Intern / DuWa**.

26) Klicken Sie auf **Übernehmen**.

27) Nur für italienische Länderinitialisierung:

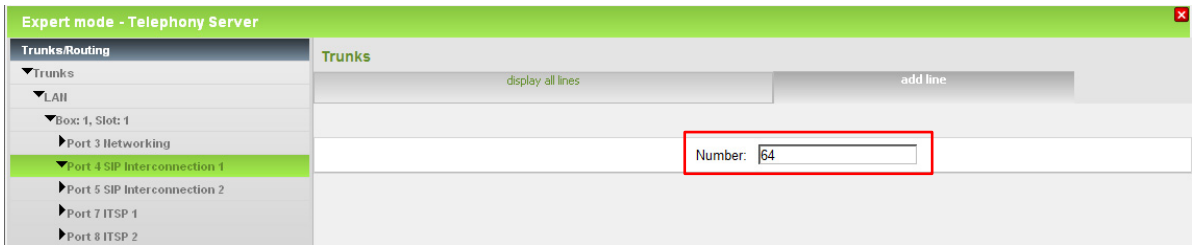
a) Klicken Sie auf die Registerkarte **Spezial Parameter ändern**.

b) Wählen Sie in der Aufklappliste **Called Party Number** den Eintrag **System-Kontrolle**.

c) Klicken Sie auf **Übernehmen**.

28) Klicken Sie im Menübaum auf **Leitungen/Vernetzung > Leitungen > LAN > Box: 1, Slot: 1 > Port 4 SIPQ-Verbindung 1**.

29) Klicken Sie auf die Registerkarte **Leitung hinzufügen**.

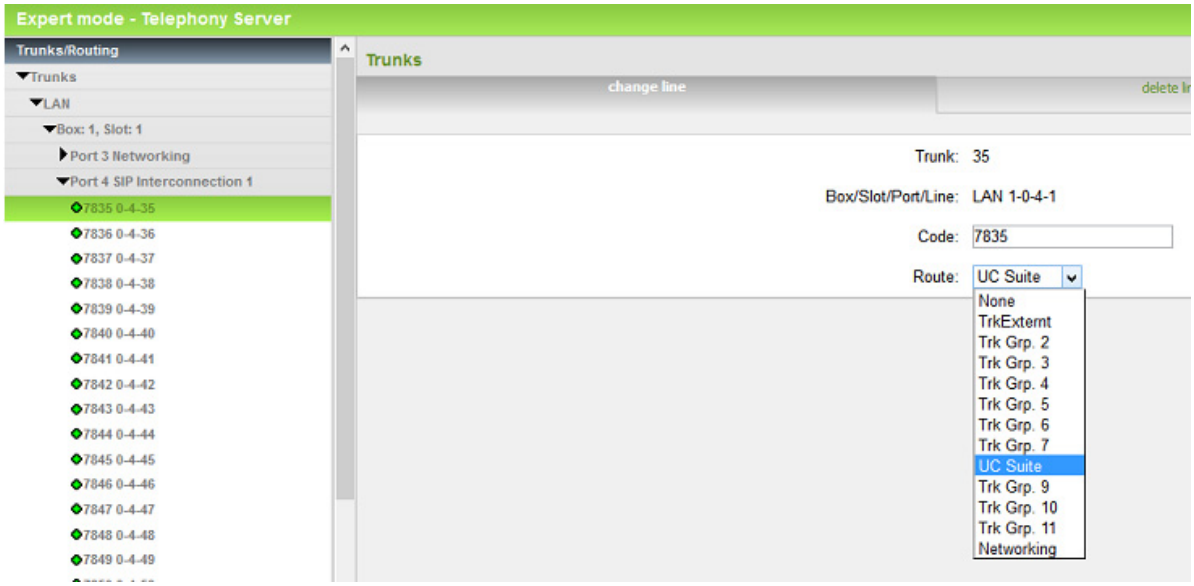


30) Geben Sie im Feld **Anzahl** den Wert `64` ein.

31) Klicken Sie auf **Übernehmen**.

32) Klicken Sie im Menübaum auf **Port 4 SIPQ-Verbindung 1**. Es werden Ihnen alle soeben eingerichteten Leitungen angezeigt.

33) Klicken Sie auf eine Leitung und wählen Sie aus der Aufklappliste **Route** die Route 8 `UC Suite` aus.

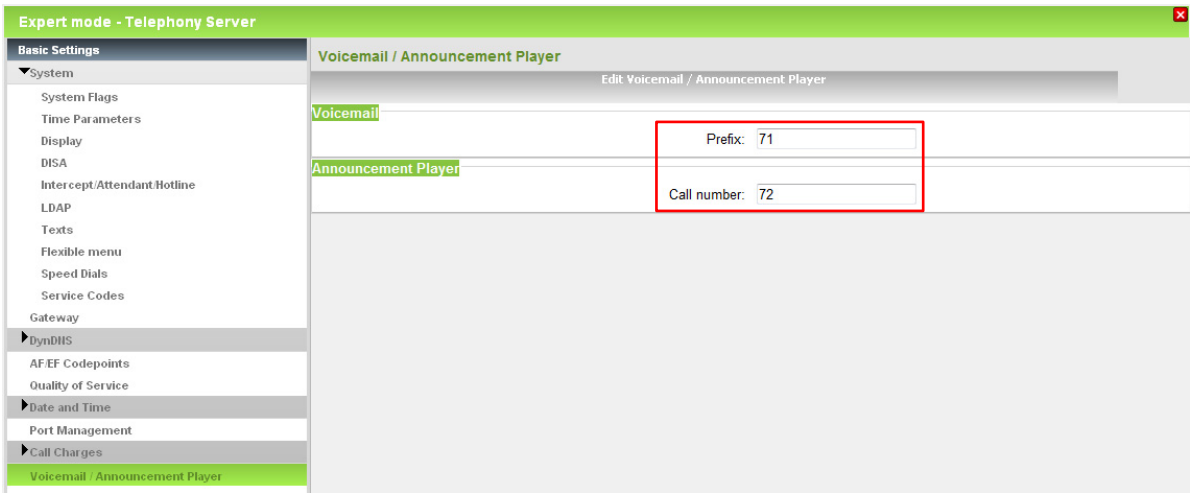


34) Klicken Sie auf **Übernehmen**.

35) Wiederholen Sie diese Zuordnung für alle benötigten Leitungen.

36) Klicken Sie im Navigationsbaum auf **Telephonie > Grundeinstellungen**.

37) Klicken Sie im Menübaum auf **Grundeinstellungen > Wiedergabegerät für Sprachnachrichten/Ansagen**.



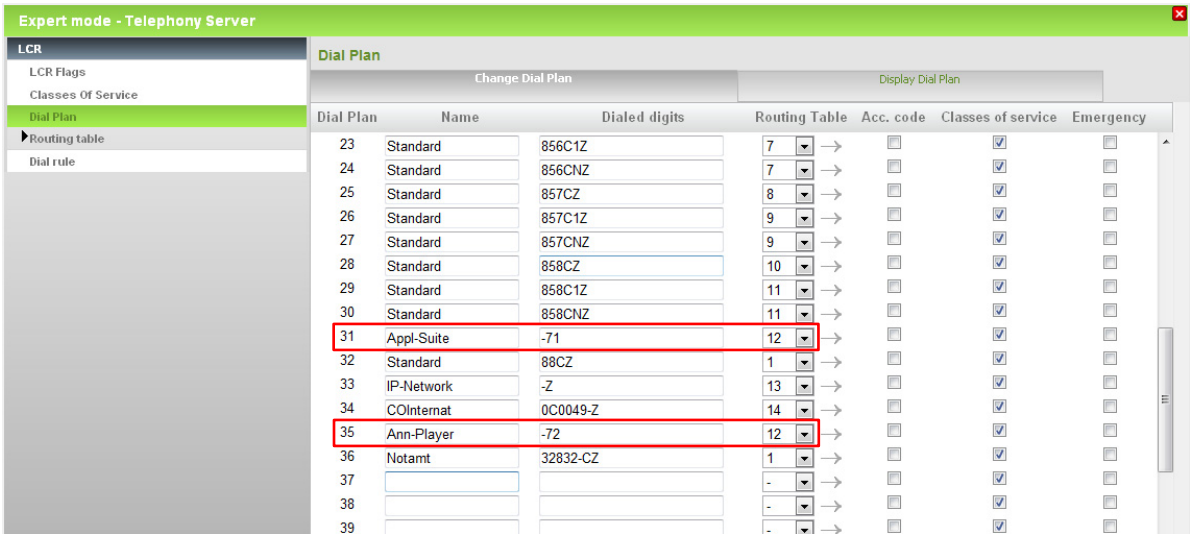
38) Geben Sie im Bereich **Voicemail** im Feld **Präfix** den Wert `71` als Standard-Rufnummer der Sprachbox ein.

39) Geben Sie im Bereich **Wiedergabegerät für Ansagen** im Feld **Rufnummer** den Wert `72` als Standard-Rufnummer den Announcement Player ein.

40) Klicken Sie auf **Übernehmen**.

41) Klicken Sie im Navigationsbaum auf **Telephonie > LCR**.

42) Klicken Sie im Menübaum auf **LCR > Wahlplan**.



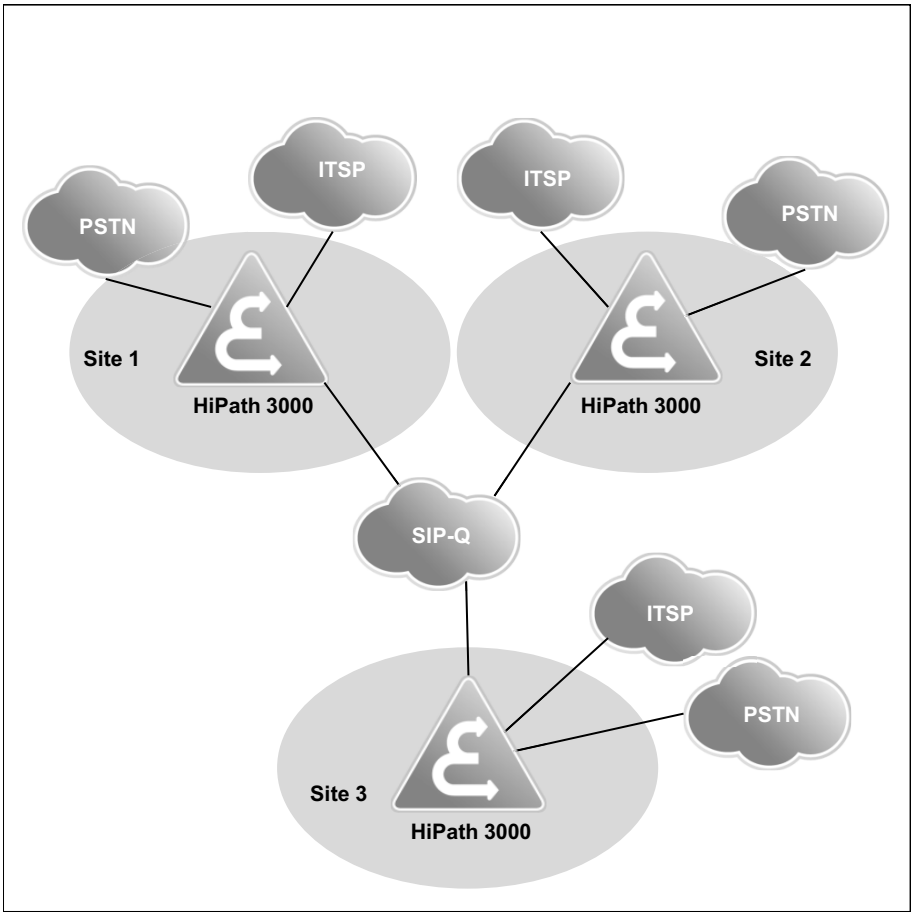
43) Wählen Sie bei Wahlplan 31 **Appl-Suite** und bei Wahlplan 35 **Ann-Player** in der Aufklappliste jeweils die Wegetabelle **12** aus.

44) Klicken Sie auf **Übernehmen**.

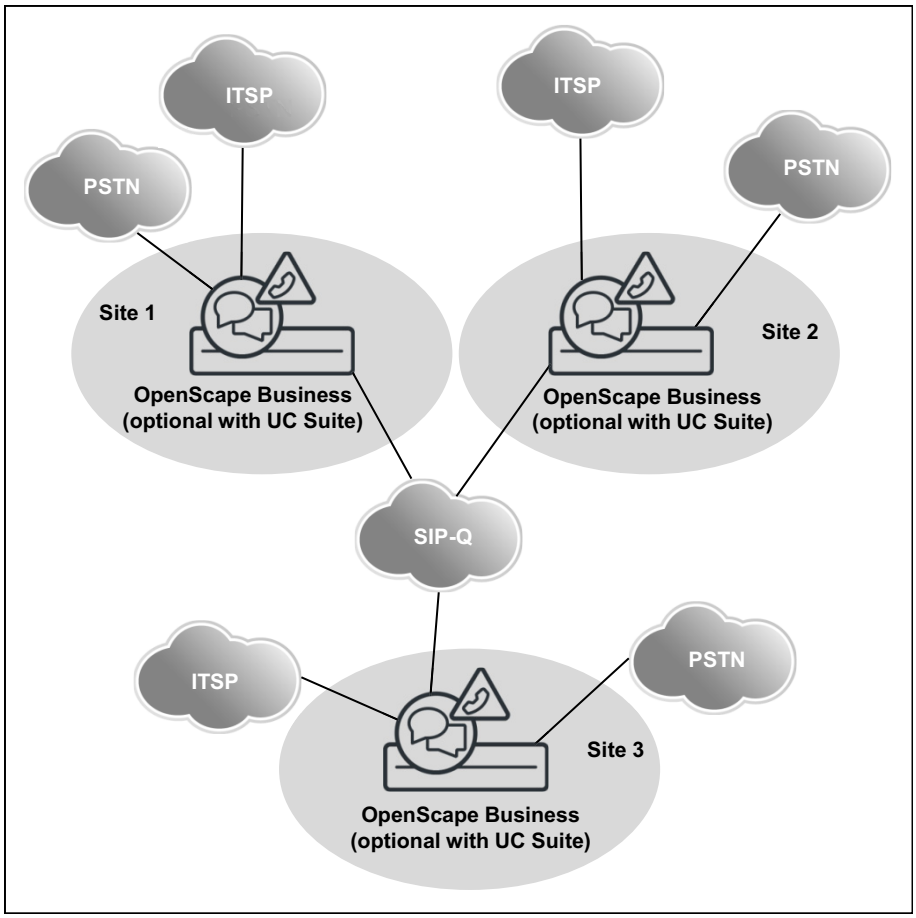
25.5 Migration eines HiPath 3000 V9 Netzverbunds

Um einen HiPath 3000 V9 Netzverbund auf einen OpenScape Business Netzverbund hochzurüsten, sind die nachstehend beschriebenen Migrationsschritte durchzuführen.

HiPath 3000 V9 Netzverbund



OpenScape Business V1 Netzverbund



Migrationsschritte

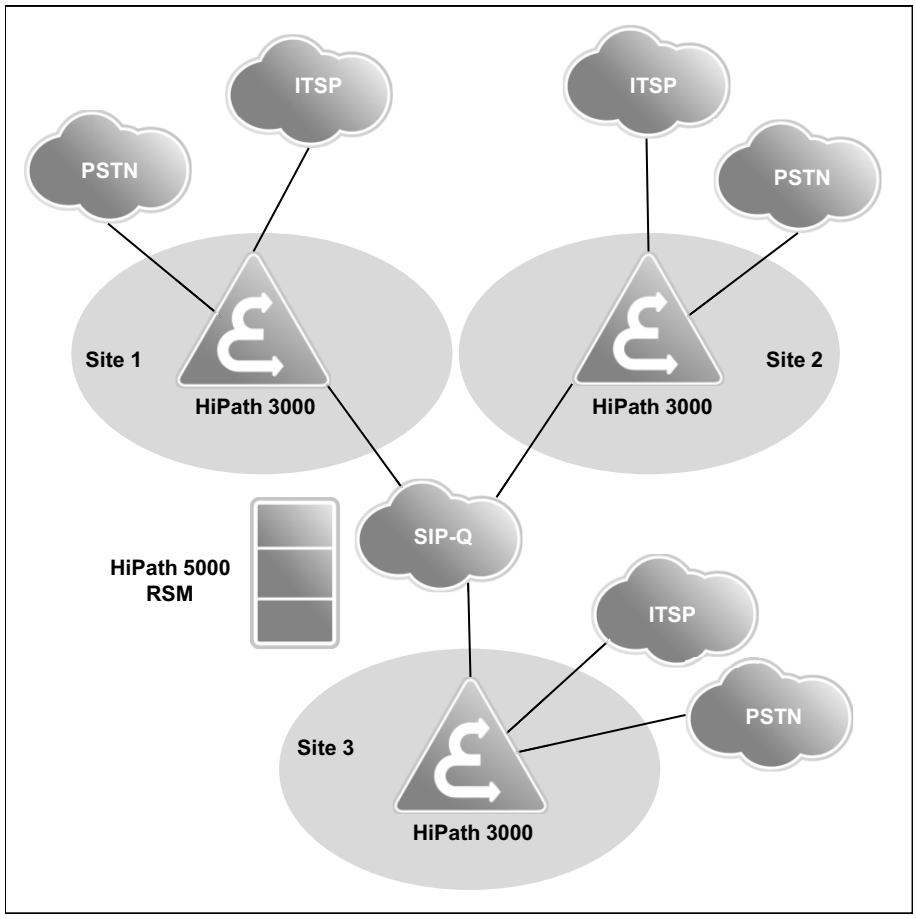
Führen Sie folgende Schritte der Reihe nach durch:

1. **HiPath 3000 V9 hochrüsten**
   Alle HiPath 3000 Systeme des Netzverbunds sind separat gemäß der Migrationsbeschreibung eines Standalone-Systems hochzurüsten.
2. **Konfiguration anpassen**
   Folgende Konfigurationsparameter sind nachträglich über den WBM-Experten-Modus anzupassen:
   - LCR-Einträge
   - Voicemail-System (Sammelanschluss, Kennzahl zur Anwahl der Voicemail)
   - Ansagen
3. **Lizenzierung durchführen**
   Nachdem alle Systeme hochgerüstet sind, erfolgt die Zusammenfassung der einzelnen Lizenz-Dateien zu einer netzweiten Lizenz am CLS.

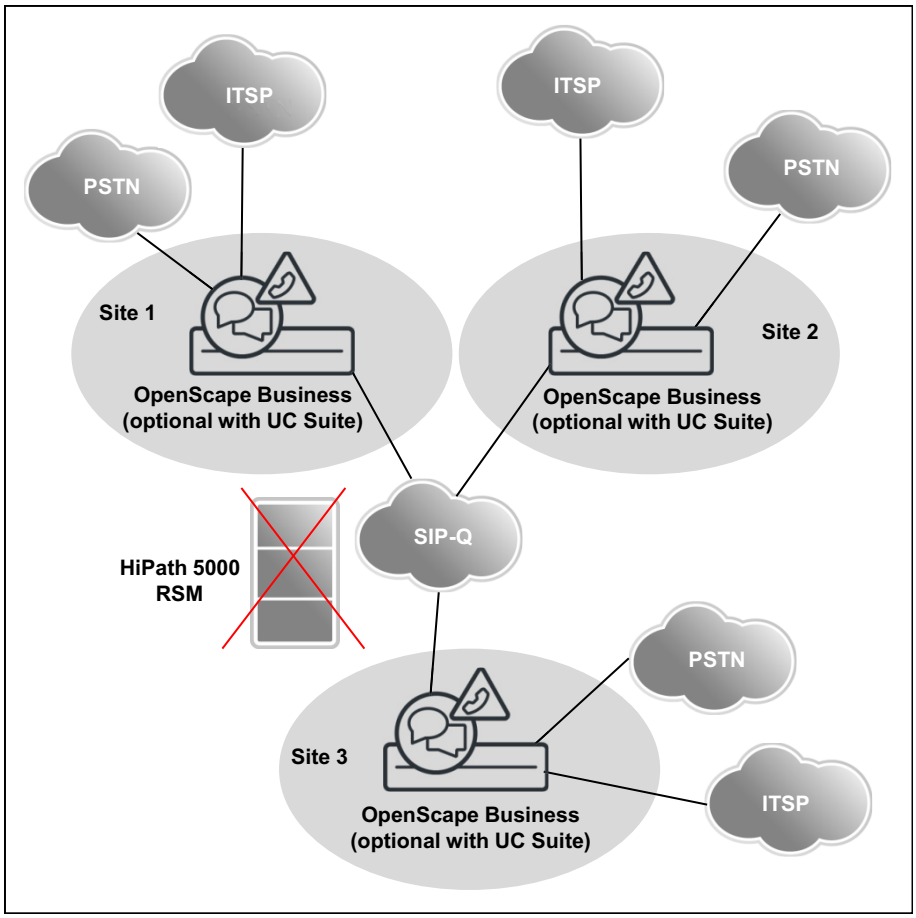
25.6 Migration eines HiPath 3000 V9 Netzverbunds mit HiPath 5000 RSM

Um einen HiPath 3000 V9 Netzverbund mit angeschlossener HiPath 5000 RSM auf einen OpenScape Business Netzverbund hochzurüsten, sind die nachstehend beschriebenen Migrationsschritte durchzuführen. Der Leistungsumfang von HiPath 5000 RSM ist in OpenScape Business integriert, somit wird HiPath 5000 RSM im OpenScape Business Netzverbund nicht mehr benötigt.

HiPath 3000 V9 Netzverbund



OpenScape Business V1 Netzverbund



Migrationsschritte

Führen Sie folgende Schritte der Reihe nach durch:

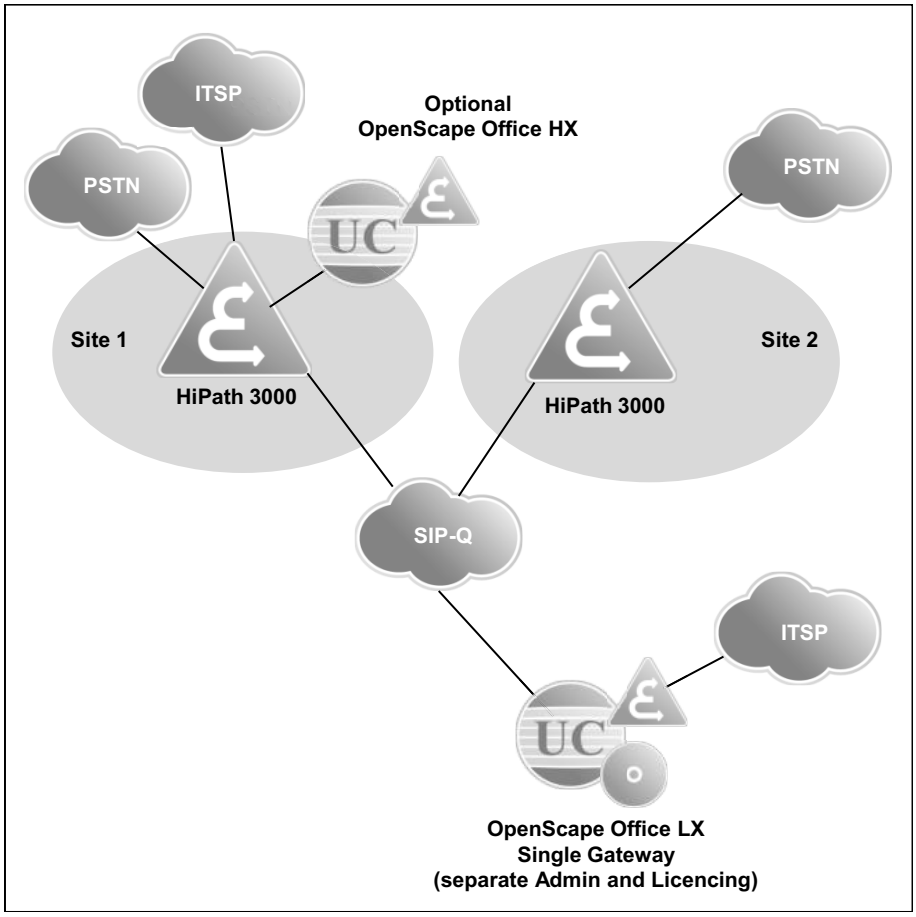
1. **Netzweite Lizenzierung auflösen**
   Ein HiPath 3000 V9 Netzverbund mit HiPath 5000 RSM nutzt die netzweite Lizenzierung. Die Netzwerklizenzdatei ist am CLS zunächst in einzelne Lizenzdateien aufzulösen und den Locking-IDs (MAC-Adressen) der HiPath 3000 V9 Systeme zuzuordnen, bevor die eigentliche Migration nach OpenScape Business beginnen kann.
   - Ordnen Sie zunächst die Lizenzen des HiPath 5000 RSM Netzverbundes den jeweiligen Locking-IDs der HiPath 3000 Knoten zu. Empfehlung: Erstellen Sie eine Excel-Liste mit entsprechender Zuordnung der jeweiligen Lizenzen zu den Locking-IDs der HiPath 3000 Systeme.
   - Kontaktieren Sie die Lizenz-Hotline, um die Aufteilung der Lizenzen gemäß Exel-Liste ausführen zu lassen.
   - Laden Sie die Einzellizenzen der HiPath 3000 Systeme zur Kontrolle vom CLS. Eine Aktivierung der Lizenzen, d. h. die Lizenz-Übertragung in die HiPath 3000 Systeme ist nicht erforderlich.

2. **HiPath 5000 RSM entfernen**
   Vor der Hochrüstung der HiPath 3000 Systeme wird HiPath 5000 RSM abgeschaltet.
3. **HiPath 3000 V9 hochrüsten**
   Alle HiPath 3000 Systeme des Netzverbunds sind separat gemäß der Migrationsbeschreibung eines Standalone-Systems hochzurüsten.
4. **Konfiguration anpassen**
   Folgende Konfigurationsparameter sind nachträglich über den WBM-Experten-Modus anzupassen:
   - LCR-Einträge
   - Voicemail-System (Sammelanschluss, Kennzahl zur Anwahl der Voicemail)
   - Ansagen
5. **Lizenzierung durchführen**
   Nachdem alle Systeme hochgerüstet sind, erfolgt die Zusammenfassung der einzelnen Lizenz-Dateien zu einer netzweiten Lizenz am CLS.

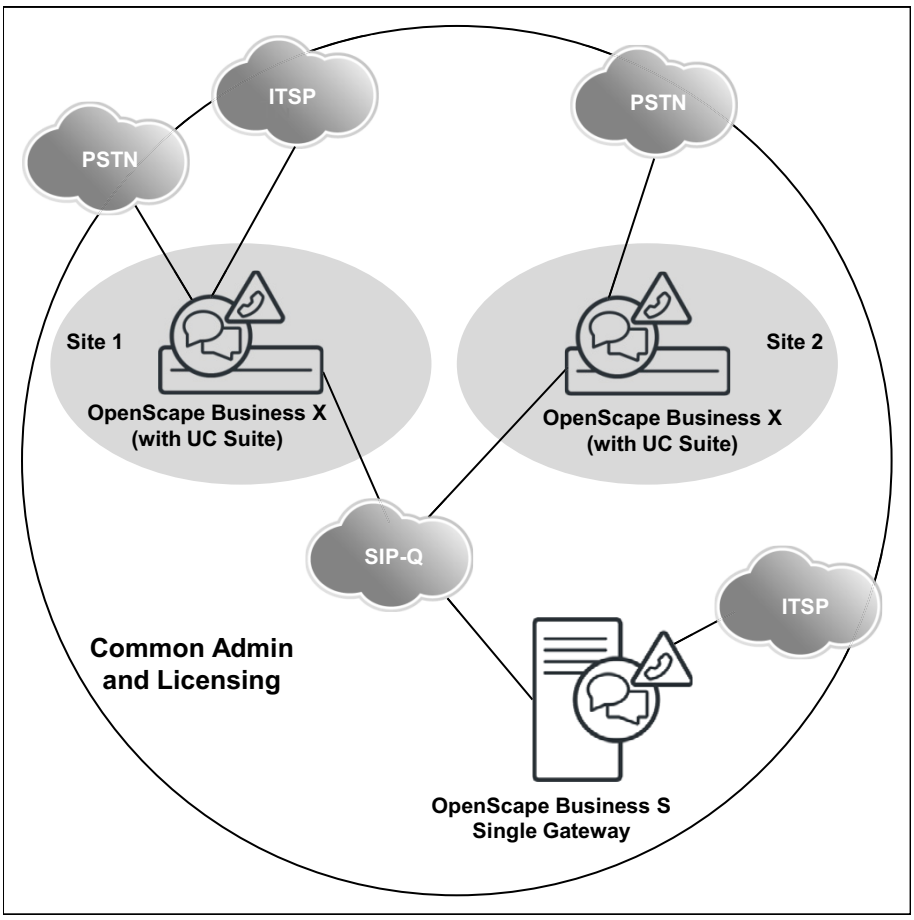
25.7 Migration eines HiPath 3000 V9 Netzverbunds mit OpenScape Office LX

Um einen HiPath 3000 V9 Netzverbund mit angeschlossener OpenScape Office LX auf einen OpenScape Business Netzverbund mit angeschlossener OpenScape Business S hochzurüsten, sind die nachstehend beschriebenen Migrationsschritte durchzuführen.

HiPath 3000 V9 Netzverbund



OpenScape Business V1 Netzverbund



Migrationsschritte

Führen Sie folgende Schritte der Reihe nach durch:

1. **HiPath 3000 V9 hochrüsten**
   Alle HiPath 3000 Systeme des Netzverbunds sind separat gemäß der Migrationsbeschreibung eines Standalone-Systems hochzurüsten.
2. **Konfiguration anpassen**
   Folgende Konfigurationsparameter sind nachträglich über den WBM-Experten-Modus anzupassen:
   - LCR-Einträge
   - Voicemail-System (Sammelanschluss, Kennzahl zur Anwahl der Voicemail)
   - Ansagen
3. **Lizenzierung durchführen**
   Es ist eine Upgrade-Lizenz von OpenScape Office LX nach OpenScape Business S zu erwerben. Nachdem alle Systeme hochgerüstet sind, erfolgt die Zusammenfassung der einzelnen Lizenz-Dateien zu einer netzweiten Lizenz am CLS.

4. **OpenScape Business S installieren und konfigurieren**
   Für OpenScape Business S wird auf einem Server-PC das Linux-Betriebssystem SLES 11 SP3 64 Bit installiert und anschließend die Kommunikationssoftware. Details finden Sie in der Installationsanleitung OpenScape Business V1, Linux-Server.
   Die Konfigurationsdaten von OpenScape Office LX können nicht übernommen werden. Daher muss die OpenScape Business S im WBM neu konfiguriert werden.
5. **Communications Clients und Application Launcher neu installieren**
   Die Communications Clients (wie z. B. myPortal for Desktop, myPortal for Outlook, ...) und der Application Launcher müssen deinstalliert und anschließend wieder neu installiert werden. Die Deinstallation und Installation ist in den Bedienungsanleitungen der Communications Clients beschrieben.

25.8 Geänderte Leistungsmerkmale und Schnittstellen

Einige HiPath 3000 Leistungsmerkmale und Schnittstellen sind für OpenScape Business in ihrer Funktion angepasst und erweitert worden.

SDHC-Kartentausch

Der Austausch der SDHC-Karte bei eingeschaltetem System (bei HiPath 3000 als Speed-Update bekannt) ist aus technischen Gründen nicht möglich. Ferner kann die SDHC-Karte eines lizenzierten Systems A nicht für ein anderes System B verwendet werden, da die Lizenzierung an die Locking-ID des Mainboards A gebunden ist. Soll die SDHC-Karte im System B eingesetzt werden, muss sie mit dem Card Manager mit einer neuen Software beschrieben werden.

Erweiterung der SIP-Funktionalität

Folgende SIP-Leistungsmerkmale sind gegenüber HiPath 3000 V9 zusätzlich implementiert:

- Call completed elsewhere
- Message Waiting Indication for Voicemail
- Calling Name Presentation (CNIP)
- Distinctive Ringing (internal/external calls)
- 3rd Party Call Control
- Call Forwarding busy/no reply/unconditional (handset controlled)

Erweiterung von SIP-Trunking

Zur Anbindung externer SIP-Server (z. B. OpenScape Alarm Server, OpenScape 4000/HiPath 4000, OpenScape Voice oder UC-Suite) stehen in OpenScape Business zwei SIP-Richtungen zur Verfügung (bei HiPath 3000 nur eine SIP-Richtung). Damit sind zusätzlich zu den klassischen Richtungen für Amt, Vernetzung und ITSP zwei unabhängige SIP-Trunk-Schnittstellen für zertifizierte SIP-Applikationen vorgesehen (SIP-Interconnection genannt).

Siehe *Vernetzung von OpenScape Business*

LCR

Die Wegetabellen 1 bis 15 sind für Default-Einträge bzw. für eine Konfiguration über Wizards vorgesehen. Bei einer Migration werden die in HiPath 3000 vorhandenen Einträge in diese Wegetabellen nicht übernommen. Eine manuelle Nachbearbeitung der Wegetabellen ist erforderlich.

Automatische Leitungsbelegung

Es kann entweder die Funktion "LCR" oder die Funktion "Automatische Leitungsbelegung (Vereinfachte Wahl)" aktiviert sein. Deshalb wird bei der Migration automatisch "LCR" aktiviert und "Automatische Leitungsbelegung (Vereinfachte Wahl)" deaktiviert. Soll aber "LCR" deaktiviert und "Automatische Leitungsbelegung (Vereinfachte Wahl)" aktiviert werden, muss zuerst der Wizard "Basisinstallation" durchlaufen werden und anschließend können die Flags mit dem Manager E entsprechend gesetzt werden (nicht für OpenScape Business X1, da hier keine Administration über den Manager E möglich ist).

VoIP over PPP via ISDN

Geroutete Sprachverbindungen über Leitungen mit geringer Bandbreite werden nicht mehr unterstützt

G.723-Unterstützung

G.723-Codecs werden nicht mehr unterstützt.

Babyphone (Raumüberwachung)

Das Leistungsmerkmal "Babyphone (Raumüberwachung)" wird nicht mehr unterstützt. Da die Funktion "CSTA-Monitoring" immer aktiv ist (ein Systemtelefon kann von einer Applikation - z. B. myAgent, myPortal - überwacht werden), kann die Funktion "Raumüberwachung" für dieses Systemtelefon nicht mehr aktiviert werden. Während der KDS-Konvertierung mit dem Manager E wird die Kennzahl für die Aktivierung der Raumüberwachung gelöscht.

Anzahl der Basisstationen und DECT-Telefone an OpenScape Business X3

Die Anzahl der Basisstationen an OpenScape Business X3 wurde gegenüber HiPath 33xx von 3 auf 7 erhöht. Die Anzahl der DECT-Telefone an OpenScape Business X3 wurde gegenüber HiPath 33xx von 16 auf 32 erhöht.

entry Web Services

Die entry Web Services werden nicht mehr unterstützt. Der Nachfolger von myPortal entry nennt sich myPortal Smart und bietet einen erweiterten Funktionsumfang. myPortal for Mobile steht weiterhin zur Verfügung. Für den Einsatz von myPortal for Mobile und myPortal Smart ist der Plug PC nicht mehr nötig.

OpenStage GateView auf Basis des Plug PC

OpenStage Gate View kann auf dem Plug PC weiterhin betrieben werden. Die Einstellungen bzgl. der OpenStage Telefone sollten überprüft werden.

SSDP auf Basis des Plug PC

SSDP ist in OpenScape Business intergriert. Der Plug PC ist nicht mehr nötig.

Externe Voicemail

Wird bei HiPath 3000 für die Voicemail weder die EVM noch die IVM verwendet, sondern eine externe Voicemail wie z. B. Xpressions, OpenScape Office HX oder eine IVM eines anderen Knotens, müssen nach der KDS-Konvertierung die 10 EVM-Ports im Manager E von "Phonemail" auf "Standard" gesetzt werden.

CSTA-Applikationen

Zur Anbindung von CSTA-Applikationen ist eine UC Booster Card oder ein UC Booster Server erforderlich. In einem Netzverbund muss an mindestens einem Knoten eine UC Booster Card oder ein UC Booster Server vorhanden sein. Die Applikationen müssen CSTAv3-Protokoll unterstützen. Gegenüber HiPath 3000 V9 sind Änderungen des CSTA-Protokolls implementiert. Daher sind CSTA-Applikationen an HiPath 3000 V9 ggf. nicht kompatibel einsetzbar an OpenScape Business. CSTAv2-Protokoll wird nicht mehr unterstützt. Eine Lizenz wird für die CSTA-Schnittstelle nicht benötigt.

Für die OpenScape Business V1 CSTA-Schnittstelle gelten im Vergleich zur HiPath 3000 CSTA-Schnittstelle die nachfolgend beschriebenen Änderungen.

- Das CSTA-Protokoll ist ausschließlich für Ethernet-LAN-Verbindungen verfügbar. Der Zugang erfolgt über Port 8800 (Standard). RS-232- und S0-Schnittstellen werden nicht mehr unterstützt.
- Für die CSTA-Schnittstelle wird keine Lizenz benötigt.
- Bevor die CSTA Schnittstelle genutzt werden kann, müssen die CSTA-Anmeldeinformationen individuell konfiguriert werden. Werksvoreinstellungen werden nicht mehr implementiert.
- Die Flags für CSTA-Plus-Produkte sind wie folgt voreingestellt und können nicht geändert werden:
  - Richtungspräfixe werden immer mit der Rufnummer übertragen
  - Erweitertes CSTA-CAUSE-Handling" ist immer aktiviert
  - CSTA-CSP-Signalisierung ist immer aktiviert
  - MULAP Monitoring ist immer aktiviert
  - CTI Networking ist immer aktiviert
  - Das OpenScape Contact Center-Flag ist immer aktiviert
- Für externe Applikationen stehen max. 4 CSTA-Verbindungen zur Verfügung. Ab Werk ist immer eine CSTA-Verbindung aktiviert. Bis zu drei weitere CSTA-Verbindungen sind optional aktivierbar, sofern diese nicht von Embedded-Applikationen des Systems verwendet werden.
- Die CSTA Phase II Protokollversion wird nicht mehr unterstützt.

Technische Details siehe:

- *Application Connectivity*
- `http://wiki.unify.com/wiki/OpenScape_Business`

TAPI 120/170 V2

Für TAPI 120/170 V2 können die bestehenden Lizenzen nicht übernommen werden. Es müssen neue Lizenzen gekauft werden. TAPI 120/170 V2 muss deinstalliert und dafür OpenScape Business TAPI 120/170 V1 neu installiert und konfiguriert werden. TAPI-Lizenzen sind in OpenScape Business userbezogen einrichtbar, daher entfällt die TAPI-Lizenzierung innerhalb der TAPI-Einrichtung. Die Lizenzierung ist ab dem ersten TAPI-User erforderlich. (auch TAPI120 ist damit nicht mehr lizenzfrei für die ersten 6 User) Der CMD (CSTA-Message Dispatcher) ist in OpenScape Business integriert. Ein separater Windows-Server für den CMD ist daher nicht mehr erforderlich. Die Anbindung von externen TAPI-Applikationen ist sowohl bei OpenScape Business als auch bei OpenScape Business S möglich. Für OpenScape Business ist zusätzlich eine UC Booster Card oder ein UC Booster Server erforderlich. In einem Netzverbund muss entweder eine OpenScape Business S vorhanden sein oder an mindestens einem Knoten eine UC Booster Card oder ein UC Booster Server.

Für OpenScape Business TAPI 120/170 V2 V1 gelten im Vergleich zu HiPath TAPI 120/170 V2 die nachfolgend beschriebenen Änderungen.

- Der Zugang zum System erfolgt ausschließlich über Ethernet-LAN. RS-232- und S0-Schnittstellen werden nicht mehr unterstützt.
- Neue gemeinsame TAPI-Lizenz auf "pro Benutzer"-Basis für TAPI 120 TSP und TAPI 170 TSP.
- Die Lizenzen sind an die Locking-ID von OpenScape Business gebunden.
- Bestehende HiPath TAPI 120 TSP oder HiPath TAPI 170 TSP Benutzerlizenzen werden von dem neuen Lizenzierungsmechanismus nicht unterstützt.
- Keine Abwärtskompatibilität mit HiPath 3000 V8 oder V9
- Für TAPI 170 TSP gilt:
  - Der Zugang zum System erfolgt standardmäßig über den Port 8800.
  - Die Konfiguration der CSTA-Anmeldeinformationen im Setup-Dialog ist obligatorisch.
  - Multi-Node-Unterstützung im Netzwerk über den CSP des zentralen Master-Knotens.
- Für TAPI 120 TSP gilt:
  - Der Zugang zum System erfolgt standardmäßig über den Port 8900.
  - Single-Node-Unterstützung, auch bei Anbindung an den Master-Knoten eines Netzwerks.

Technische Details siehe:

- *Application Connectivity*

Accounting-Schnittstelle

Die Schnittstellen der Accounting-Daten sind gegenüber HiPath 3000 geändert.

V24-Applikationen

V24-Applikationen werden nicht mehr unterstützt.

Weitere externe Applikationen

Bitte beachten Sie für extern angeschlossene Applikationen die Hinweise und Einschränkungen in der Freigabemitteilung (Release Note).

HiPath 5000 RSM

HiPath 5000 RSM wird nicht mehr unterstützt. Die Funktionalität von HiPath 5000 RSM wurde in OpenScape Business integriert. Damit ist kein separater Server mehr erforderlich.

Leistungsmerkmal	HiPath 5000 RSM	OpenScape Business
netzweite Lizenzierung, Zuordnung der Lizenzen zu den einzelnen Knoten	Alle System-Lizenzen des Netzes am CLS zu einer netzweiten Lizenz zusammengefasst.	Alle System-Lizenzen des Netzes werden am CLS zu einer netzweiten Lizenz zusammengefasst.
netzweite Administration	DB-Feature Server: Per Manager E werden alle Knoten des Netzes zu einem Netz-KDS zusammengefasst. Der Rufnummernhaushalt wird netzweit synchronisiert.	Per WBM werden alle Knoten des Netzes mit einem Netzwerk-Wizard erfasst. Der Rufnummernhaushalt wird netzweit synchronisiert (geschlossene Nummerierung).
Anbindung an Fremd-Knoten bzw. Fremd-Applikationen	SIP-Q-Anbindung von bis zu 4 Fremd-Knoten	Bis zu 2 SIP-Interconnection-Richtungen mit SIP-Q bzw. Native SIP
Resillience / Survivability	User-Survivability für HFA-Telefone bei geschlossener Nummerierung	User-Survivability für HFA-Telefone bei geschlossener Nummerierung (Wechsel von OSBiz S <--> OSBiz X3/X5/X8)
Backup / Restore	netzweit	lokal
Inventory-Funktion	netzweit	lokal

Leistungsmerkmal	HiPath 5000 RSM	OpenScape Business
Presence Manager	netzweite Funktion mit der Bereitstellung von 5000 RSM	netzweite Funktion mit Bereitstellung eines Multi-node-CSP auf Basis von OSBiz UC Booster Card oder OSBiz UC Booster Server oder OSBiz S
TAPI 170 am Standalone-System	TAPI 170 am Standalone-System läuft auf einem Windows-PC mit eigener Lizenzierung (separates Lizenzfile für den TAPI 170).	TAPI 170 am Standalone-System läuft auf einem Windows-PC. Die Lizenzabfrage und Versorgung der TAPI 170 Database erfolgen aus der SQL-DB von OSBiz. Die Anbindung des TAPI 170 erfolgt über den CSP des Systems. (OSBiz UC Booster Card, OSBiz UC Booster Server oder OSBiz S)
TAPI 170 im Netzverbund	TAPI 170 läuft auf 5000 RSM mit eigener Lizenzierung(separates Lizenzfile für den TAPI 170). Die TAPI 170 Database wird aus dem DB-Feature Server von 5000 RSM bezogen.	wie am Standalone-System, jedoch erfolgt die Anbindung des TAPI 170 am Multi-Node-CSP des Master-Knotens (d.h. netzweit).

Gemischte Netze

Ein gemischter Netzverbund aus OpenScape Business und OpenScape Office wird nicht unterstützt.

25.9 Nicht unterstützte Baugruppen und Endgeräte

Einige Baugruppen und Endgeräte können aus technischen Gründen nicht in den Kommunikationssystemen OpenScape Business X3/X5/X8 eingesetzt werden.

Bei einer Migration von HiPath 3000 V9 nach OpenScape Business V1 sind diese Baugruppen und Endgeräte zu entfernen. Bei Bedarf kann stattdessen der jeweilige Nachfolger eingesetzt werden.

Baugruppe/ Gerät	Sachnummer	Einsatz in	Funktion	Hinweise / Nachfolger
ALUM4	S30817-Q935-A	X3W X5W	Umschaltung von bis zu 4 analogen Amtsleitungen auf bis zu 4 analoge Telefone bei Netzspannungsausfall	ALUM4 muss entfernt werden. TLANI2 (S30810-Q2953-Xxxx) und TLANI4 (S30810-Q2953-Xxxx) stellen jeweils 2 Amtsleitungsumschaltungen zur Verfügung.
ANI	S30807-Q6917-A103	X3W X5W	Bereitstellung von CLIP für bis zu 4 Amtsleitungen	ANI muss entfernt werden. CLIP-Funktion integriert auf TLANI2 (S30810-Q2953-Xxxx), TLANI4 (S30810-Q2953-Xxxx) und TLANI8 (S30810-Q2954-Xxxx)
ANIR	S30807-Q6917-Z103	X3R X5R	Bereitstellung von CLIP für bis zu 4 Amtsleitungen	ANIR muss entfernt werden. CLIP-Funktion integriert auf TLANI4R (S30810-K2953-Xxxx)
CBCC	S30810-Q2935-Axxx	X3W X5W	Mainboard (zentrale Steuerung)	CBCC muss entfernt werden. OCCM (S30810-Q2959-X)
CBRC	S30810-Q2935-Zxxx	X3R X5R	Mainboard (zentrale Steuerung)	CBRC muss entfernt werden. OCCMR (S30810-K2959-Z)
CBSAP	S30810-Q2314-X	X8	Mainboard (zentrale Steuerung)	CBSAP muss entfernt werden. OCCL (S30810-Q2962-X)
CMS	S30807-Q6928-X	X3R X3W X5R X5W X8	Bereitstellung eines hochgenauen Taktes	CMS muss entfernt werden. Funktionalität integriert auf OCCL/OCCM/OCCMR
EVM	S30807-Q6945-X	X3R X3W X5R X5W	Bereitstellung von VoiceMail	EVM muss entfernt werden. Funktionalität integriert auf OCCL/OCCM/OCCMR
EXMNA (nur für USA)	S30807-Q6923-X	X3W X5W	Ermöglicht die Anschaltung einer externen Musikquelle	EXMNA muss entfernt werden. Einsatz einer anderen Option für die Anschaltung einer externen Musikquelle erforderlich

Baugruppe/ Gerät	Sachnummer	Einsatz in	Funktion	Hinweise / Nachfolger
GEE12 GEE16 GEE50	S30817-Q951-Axxx	X3W X5W	Gebührenerfassung mit 12 kHz/16 kHz/50 Hz-Impulsen für bis zu 4 Amtsleitungen	GEE12, GEE16 und GEE50 müssen entfernt werden. Gebührenerfassung integriert auf TLANI2 (S30810-Q2953-Xxxx), TLANI4 (S30810-Q2953-Xxxx) und TLANI8 (S30810-Q2954-Xxxx)
HOPE	S30122-Q7078-X S30122-Q7079-X	X3W X5W	Bereitstellung von Hicom Office PhoneMail Entry	HOPE muss entfernt werden. Einsatz einer anderen Voice-Mail erforderlich.
HXGR3	S30810-K2943-Z1	X3R X5R	HG1500-Baugruppe	HXGR3 muss entfernt werden. Funktionalität integriert auf OCCMR
HXGS3	S30810-Q2943-X1	X3W X5W	HG1500-Baugruppe	HXGS3 muss entfernt werden. Funktionalität integriert auf OCCM
IMODN	S30807-Q6932-X100	X3R X3W X5R X5W X8	Analoges Modem	IMODN muss entfernt werden. Funktionalität steht nicht mehr zur Verfügung.
LIM	S30807-Q6930-X	X3R X3W X5R X5W	Bereitstellung einer LAN-Schnittstelle	LIM muss entfernt werden. Funktionalität integriert auf OCCM/OCCMR
LIMS	S30807-Q6721-X	X8	Bereitstellung von zwei LAN-Schnittstellen	LIMS muss entfernt werden. Funktionalität integriert auf OCCL
LUNA2	S30122-K7686-A1-3 oder niedriger S30122-K7686-A1-B1 oder niedriger S30122-K7686-M1-9 oder niedriger	X8	Stromversorgung	Ältere LUNA2 müssen entfernt werden. Nachfolgebaugruppen: S30122-K7686-A1-4 oder höher S30122-K7686-A1-C1 oder höher S30122-K7686-M1-10 oder höher

Baugruppe/ Gerät	Sachnummer	Einsatz in	Funktion	Hinweise / Nachfolger
MMP3	S30122-K7730-X	X3W X5W	MP3-Player für Wartemusik (Musik On Hold), A-law Version	MMP3 muss entfernt werden. Einsatz eines anderen MP3-Players für Wartemusik erforderlich
MUSIC Einsteckmodul	S30122-K5380-T200	X3W X5W	Bereitstellung von Wartemusik (Musik On Hold)	MUSIC Einsteckmodul muss entfernt werden. Einsatz einer anderen Option für die Bereitstellung von Wartemusik erforderlich
PBXXX	S30810-Q6401-X	X8	CAS-Protokollkonverter für 1 S_{2M}-Schnittstelle	PBXXX muss entfernt werden. CAS-Protokollkonverter integriert auf TMCAS2 (S30810-Q2946-X)
PDM1	S30807-Q5692-X100	X3R X3W X5R X5W	Bereitstellung von einem DSP (Digital Signal Processor)	PDM1 muss entfernt werden. OCCB1 (S30807-Q6949-X100) oder OCCB3 (S30807-Q6949-X)
PSU C	S30122-K5661-*	X5	Stromversorgung	PSU C muss entfernt werden. UPSC-D (S30122-K5660-A300) UPSC-DR (S30122-K7373-A900)
PSU P	S30122-K5658-*	X3	Stromversorgung	PSU P muss entfernt werden. UPSC-D (S30122-K5660-A300) UPSC-DR (S30122-K7373-A900)
STBG Nur für Frankreich	S30817-Q934-A	X3W X5W	Strombegrenzung für bis zu 4 Amtsleitungen	STBG muss entfernt werden. Keine Nachfolge-Baugruppe
STMI2	S30810-Q2316-X100	X8	HG1500-Baugruppe	STMI2 muss entfernt werden. Funktionalität integriert auf OCCL
TLA2	S30817-Q923-Bxxx	X3W X5W	Analoge Amtsbaugruppe mit 2 a/b-Schnittstellen	TLA2 muss entfernt werden. TLANI2 (S30810-Q2953-Xxxx)
TLA4	S30817-Q923-Axxx	X3W X5W	Analoge Amtsbaugruppe mit 4 a/b-Schnittstellen	TLA4 muss entfernt werden. TLANI4 (S30810-Q2953-Xxxx)

Baugruppe/ Gerät	Sachnummer	Einsatz in	Funktion	Hinweise / Nachfolger
TLA4R	S30817-K923-Zxxx	X3R X5R	Analog trunk line with ALUM, 4 ports	TLA4R muss entfernt werden. TLANI4R (S30810-K2953-Xxxx)
TLA8	S30817-Q926-Axxx	X3W X5W	Analoge Amtsbaugruppe mit 8 a/b-Schnittstellen	TLA8 muss entfernt werden. TLANI8 (S30810-Q2954-Xxxx)
TMDID	S30810-Q2452-X	X8	Analoge Amtsbaugruppe mit 8 a/b-Schnittstellen	TMDID muss entfernt werden. TMDID (S30810-Q2197-T)
TMGL2	S30810-Q2918-X100	X3W X5W	Analoge Amtsbaugruppe mit 2 a/b-Schnittstellen	TMGL2 muss entfernt werden. TLANI2 (S30810-Q2953-Xxxx)
TMGL4	S30810-Q2918-X	X3W X5W	Analoge Amtsbaugruppe mit 4 a/b-Schnittstellen	TMGL4 muss entfernt werden. TLANI4 (S30810-Q2953-Xxxx)
TMGL4R	S30810-Q2918-Z	X3R X5R	Analoge Amtsbaugruppe mit 4 a/b-Schnittstellen	TMGL4R muss entfernt werden. TLANI4R (S30810-K2953-Xxxx)
TMQ4 Nur für USA	S30810-Q2917-X	X3W X5W	Digitale Amtsbaugruppe mit 4 S_0-Schnittstellen	TMQ4 muss entfernt werden. Keine Nachfolge-Baugruppe
TS2	S30810-Q2913-X100	X5W	Digitale Amts-/Querverkehr-baugruppe mit 1 S_{2M}-Schnitt-stelle	TS2 muss entfernt werden. TS2N (S30810-Q2913-X300)
TS2R	S30810-K2913-Z100	X5R	Digitale Amts-/Querverkehr-baugruppe mit 1 S_{2M}-Schnitt-stelle	TS2R muss entfernt werden. TS2RN (S30810-K2913-Z300)
UAM	S30122-K7217-T	X3W X5W	Bereitstellung von Music On Hold (MoH)	UAM muss entfernt werden. Funktionalität wird durch Soft-ware realisiert
UAMR	S30122-K7402-T	X3R X5R	Bereitstellung von Music On Hold (MoH)	UAMR muss entfernt werden. Funktionalität wird durch Soft-ware realisiert

Baugruppe/ Gerät	Sachnummer	Einsatz in	Funktion	Hinweise / Nachfolger
V24/1	S30807-Q6916-X100	X3W X5W	Bereitstellung einer V.24-Schnittstelle	V24/1 muss entfernt werden. Keine Nachfolge-Baugruppe
optiset Telefone und optiset E Telefone	---	X3R X3W X5R X5W X8	UP0-Telefon	optiset und optiset E Telefone können sich nicht mehr an OpenScape Business anmelden OpenStage T
optiPoint WL2 professional HFA-Version	---	X3R X3W X5R X5W X8	WLAN-Telefon	optiPoint WL2 professional SIP-Version

optiPoint WL2 professional

Das Telefon optiPoint WL2 professional wird in der HFA-Variante nicht von OpenScape Business unterstützt. Deshalb ist es von der HFA-Variante auf die SIP-Variante umzurüsten.

25.9.1 Wie Sie ein optiPoint WL2 professional von HFA auf SIP umrüsten

Voraussetzungen

- Die Telefon-Software liegt als Image-Datei in der Zwischenversion `prep70_39.img` vor.
- Die Telefon-Software liegt als Image-Datei in der endgültigen Version vor, z. B. Standard-Image-Datei `swup_70-000-52.img`.
- Die Benutzerdaten des WL2 und die WLAN-Zugangsdaten liegen Ihnen vor.
- Ein neuer SIP-Teilnehmer wurde im WBM des Systems inkl. der SIP-Zugangsdaten eingerichtet und lizenziert. Die im System vergebenen SIP-Zugangsdaten liegen Ihnen vor.

Schritt für Schritt

1) Upgrade auf die Zwischenversion:

a) Installieren Sie zuerst die Zwischenversion `prep70_39.img` mittels WBM des WL2 oder DLS. Der Upgrade-Fortschritt wird auf dem Telefondisplay angezeigt.

b) Folgen sie den Anweisungen im Display und warten sie, bis das WL2 neu gestartet ist.

c) Bestätigen Sie nach erfolgreichem Start die Meldung **Temp. SW only - Please Update!** mit **OK**.

2) Upgrade auf die endgültige Version:

a) Installieren Sie nun eine Standard-Image-Datei, z. B. `swup_70-000-052.img`. Aus Sicherheitsgründen werden während des Upgrades keine Einstellungen und Benutzerdaten geändert. Der Upgrade-Fortschritt wird auf dem Telefondisplay angezeigt.

b) Folgen sie den Anweisungen im Display und warten sie, bis das WL2 neu gestartet ist.

3) Aktivieren Sie nach erfolgreichem Start die Standard-Telefoneinstellungen manuell über das WBM des WL2:

- 1. Möglichkeit: Navigieren Sie im WBM zu **System Settings > Reset User Data > User Settings Clear**.
- 2. Möglichkeit: Navigieren Sie im WBM zu **Factory Reset > Restore the factory defaults**.

HINWEIS: Ihre Benutzerdaten und die WLAN-Zugangsdaten gehen verloren!

---

4) Geben Sie die WLAN-Zugangsdaten am Telefon ein, um das Telefon ins Kunden-LAN einzubinden.

5) Geben Sie die SIP-Zugangsdaten am Telefon ein, damit sich das Telefon als SIP-Teilnehmer am System anmelden kann.

6) Setzen Sie im WBM des WL2 das Optionsfeld **Network > SIP advanced > Auto Answer** auf **On**, um die Funktionalität des Telefons im Zusammenspiel mit den UC Suite Clients sicherzustellen.

26 Ausbaugrenzen und Kapazitäten

Bei den Ausbaugrenzen und Kapazitäten handelt es sich um systembedingte Maximalwerte und um die Maximalwerte einer Vernetzung.

Die Maximalwerte beziehen sich auf

- die systembedingten Ausbaugrenzen
- die Software-Kapazitäten

26.1 Systembedingte Ausbaugrenzen

Bei den hier beschriebenen Ausbaugrenzen handelt es sich um systembedingte Maximalwerte für Teilnehmer und Leitungen.

HINWEIS: Für jede Systemkonfiguration muss geprüft werden, ob die Nennleistungsabgabe der systemeigenen Stromversorgung ausreicht oder ob eine externe Zusatzspeisung erforderlich ist (siehe *OpenScape Business V1, Montage der Hardware (Servicedokumentation)*: *Leistungsbedarf eines Kommunikationssystems*).

Maximalwerte für Teilnehmer

Teilnehmer	Maximalwerte				
	OpenScape Business				
	X1	X3R X3W	X5R X5W	X8	S
Gesamtsumme aller IP-, TDM- und Mobility Teilnehmer	30 IP/TDM plus 30 Mobility Teilnehmer	500	500	500	500
IP-Teilnehmer					
Summe der Systemtelefone, SIP-Teilnehmer, Adapter, WLAN pro Kommunikationssystem	20	500, davon sind 2 reserviert für Remote- und Serverzugriff	500, davon sind 2 reserviert für Remote- und Serverzugriff	500, davon sind 2 reserviert für Remote- und Serverzugriff	500, davon sind 2 reserviert für Remote- und Serverzugriff
TDM-Teilnehmer					
ISDN-Teilnehmer (S_0-Teilnehmer) pro Kommunikationssystem	4 (2 S_0 auf OCCS)	10 (2 S_0 auf OCCMR + 2 x STLSX4R) 10 (2 S_0 auf OCCM + 2 x STLSX4)	26 (2 S_0 auf OCCMR + 6 x STLSX4R) 26 (2 S_0 auf OCCM + 6 x STLSX4)	128	–

Teilnehmer	Maximalwerte				
	OpenScape Business				
	X1	X3R X3W	X5R X5W	X8	S
Analoge Teilnehmer pro Kommunikationssystem	4 (4 a/b auf OCCS)	20 (4 a/b auf OCCMR + 2 x SLAD8R) 20 (4 a/b auf OCCM + 1 x SLAD16)	52 (4 a/b auf OCCMR + 6 x SLAD8R) 68 (4 a/b auf OCCM + 4 x SLAD16)	384	–
$U_{P0/E}$-Teilnehmer (Master) pro Kommunikationssystem	8 (8 $U_{P0/E}$ auf OCCS)	24[1](8 $U_{P0/E}$ auf OCCMR + 2 x SLU8R) 24[1] (8 $U_{P0/E}$ auf OCCM + 2 x SLU8)	56[1] (8 $U_{P0/E}$ auf OCCMR + 6 x SLU8R) 56[1] (8 $U_{P0/E}$ auf OCCM + 6 x SLU8)	384[1]	–
Zusätzliche Teilnehmer über OpenStage PhoneAdapter ($U_{P0/E}$-Slave-Telefone, analoge Telefone)	8	24 24	56 56	116	–
Cordless-Telefone (DECT-Telefone für die integrierte Cordless-Lösung) pro Kommunikationssystem	16 (DECT Light[2])	32 (DECT Light[2])	32 (DECT Light[2]) 32 (DECT Light[2]) / 64 (1 x SLC16N)	250	–
Basisstationen (für die integrierte Cordless-Lösung) pro Kommunikationssystem	7 (Anschluss an $U_{P0/E}$ auf OCCS (DECT Light[2]))	7 (Anschluss an $U_{P0/E}$ auf OCCMR (DECT Light[2])) 7 (Anschluss an $U_{P0/E}$ auf OCCM (DECT Light[2]))	7 (Anschluss an $U_{P0/E}$ auf OCCMR (DECT Light[2])) 7 (Anschluss an $U_{P0/E}$ auf OCCM (DECT Light[2])) / 16 (Anschluss an SLC16N)[3]	64 (Anschluss an 4 x SLCN)	–
Mobility Teilnehmer					

Teilnehmer	Maximalwerte				
	OpenScape Business				
	X1	X3R X3W	X5R X5W	X8	S
Mobility: Teilnehmer pro Kommunikationssystem	30	150	150	150	–
myPortal Smart / Application Launcher: Teilnehmer pro Kommunikationssystem	30 (konfigurierbar) / 30 (gleichzeitig aktiv)	150 (konfigurierbar) / 50 (gleichzeitig aktiv)	150 (konfigurierbar) / 50 (gleichzeitig aktiv)	150 (konfigurierbar) / 50 (gleichzeitig aktiv)	–
myPortal for Mobile/Tablet (UC Smart): Teilnehmer pro Kommunikationssystem	30 (konfigurierbar) / 30 (gleichzeitig aktiv)	50 (konfigurierbar) / 30 (gleichzeitig aktiv)	50 (konfigurierbar) / 30 (gleichzeitig aktiv)	50 (konfigurierbar) / 30 (gleichzeitig aktiv)	–
myPortal for Mobile/Tablet (UC Suite): Teilnehmer pro Kommunikationssystem	30 (konfigurierbar) / 30 (gleichzeitig aktiv)	100 (konfigurierbar) / 30 (gleichzeitig aktiv)	100 (konfigurierbar) / 30 (gleichzeitig aktiv)	100 (konfigurierbar) / 30 (gleichzeitig aktiv)	200 (konfigurierbar) / 30 (gleichzeitig aktiv)
myPortal to go (UC Smart): Teilnehmer pro Kommunikationssystem	30	50	50	50	–
myPortal to go (UC Suite): Teilnehmer pro Kommunikationssystem	–	100	100	100	200 (konfigurierbar) / 100 (gleichzeitig aktiv)
Virtuelle Teilnehmer (frei konfigurierbar)	250	250	250	250	250

1 Abhängig von den Telefontypen und dem Gesamtleistungsbedarf des Kommunikationssystems.
2 Voraussetzung: CMA auf OCCMR/OCCM.
3 Der Anschluss von Basisstationen an OCCM (DECT Light) und an SLC16N innerhalb eines Kommunikationssystems ist nicht möglich.

Maximalwerte für Leitungen

Leitungen	Maximalwerte				
	OpenScape Business				
	X1	X3R X3W	X5R X5W	X8	S
Gesamtsumme aller Leitungen pro Kommunikationssystem	250 (IP- und ISDN-Leitungen)	250 (IP-, ISDN- und analoge Leitungen)	250 (IP-, ISDN- und analoge Leitungen)	250 (IP-, ISDN- und analoge Leitungen)	250 (IP-Leitungen) ISDN- und analoge Leitungen über Gateway
ISDN-Leitungen					
S_0-Leitungen	4 (2 S_0 auf OCCS)	10 (2 S_0 auf OCCMR + 2 x STLSX4R) 10 (2 S_0 auf OCCM + 2 x STLSX4)	26 (2 S_0 auf OCCMR + 6 x STLSX4R) 26 (2 S_0 auf OCCM + 6 x STLSX4)	128 (Begrenzung durch Systemsoftware)	ISDN-Leitungen über Gateway
S_{2M}-Leitungen	–	–	30 (1 x TS2RN) 30 (1 x TS2N)	180 (3 x DIUT2)	ISDN-Leitungen über Gateway
CAS-Leitungen	–	–	30 (1 x TCASR-2) 30 (1 x TCAS-2)	180 (3 x TMCAS2)	CAS-Leitungen über Gateway
Analoge Leitungen					
Analoge Leitungen	–	8 (2 x TLANI4R) 16 (2 x TLANI8)	24 (6 x TLANI4R) 48 (6 x TLANI8)	120 (15 x TMANI)	Analoge Leitungen über Gateway

Info für OpenScape Business X3/X5/X8:

Insgesamt können bis zu 250 IP-, ISDN- und analoge Leitungen genutzt werden.

Beispiele zum Maximalausbau:

- OpenScape Business X3R: 2 x TLANI4R (= 8 x a/b) = 8 analoge Leitungen + 242 IP-Leitungen
- OpenScape Business X3W: 2 x STLSX4 (= 8 x S_0) + 2 x S_0 auf OCCM = 20 B-Kanäle + 230 IP-Leitungen
- OpenScape Business X5W: 1 x TS2 (= 1 x S_{2M}) + 5 x STLSX4 (= 20 x S_0) + 2 x S_0 auf OCCM = 74 B-Kanäle + 176 IP-Leitungen
- OpenScape Business X8: 3 x DIUT2 (= 6 x S_{2M}) = 180 B-Kanäle + 70 IP-Leitungen

Maximalwerte der Ressourcen

Ressource	Maximalwerte				
	OpenScape Business				
	X1	X3R X3W	X5R X5W	X8	S
DSP-Kanäle (Gateway-Kanäle) ***Info***: Verbindungen zwischen IP- und TDM-Telefonen/-Leitungen sind sogenannte Gateway-Verbindungen, für die jeweils ein DSP-Kanal (Gateway-Kanal) benötigt wird.					
DSP-Kanäle mit aktiviertem Codec G.711	8 (auf OCCS)	8 (auf OCCMR/ OCCM)	8 (auf OCCMR/ OCCM)	8 (auf OCCL)	–
	8 (8 auf OCCS)	48 (8 auf OCCMR/OCCM + 40 auf OCCB1)	48 (8 auf OCCMR/OCCM + 40 auf OCCB1)	128 (8 auf OCCL + 120 auf OCCB3)	–
DSP-Kanäle mit aktivierten Codecs G.711 und G.729	8 (auf OCCS)	8 (auf OCCMR/ OCCM)	8 (auf OCCMR/ OCCM)	8 (auf OCCL)	–
	8 (8 auf OCCS)	40 (8 auf OCCMR/OCCM + 32 auf OCCB1)	40 (8 auf OCCMR/OCCM + 32 auf OCCB1)	104 (8 auf OCCL + 96 auf OCCB3)	–
DSP-Kanäle mit aktiviertem Codec G.711 und mit aktiviertem Leistungsmerkmal SPE	6 (auf OCCS)	6 (auf OCCMR/ OCCM)	6 (auf OCCMR/ OCCM)	6 (auf OCCL)	–
	6 (6 auf OCCS)	38 (6 auf OCCMR/OCCM + 32 auf OCCB1)	38 (6 auf OCCMR/OCCM + 32 auf OCCB1)	102 (6 auf OCCL + 96 auf OCCB3)	–
DSP-Kanäle mit aktivierten Codecs G.711 und G.729 und mit aktiviertem Leistungsmerkmal SPE	6 (auf OCCS)	6 (auf OCCMR/ OCCM)	6 (auf OCCMR/ OCCM)	6 (auf OCCL)	–
	6 (6 auf OCCS)	31 (6 auf OCCMR/OCCM + 25 auf OCCB1)	31 (6 auf OCCMR/OCCM + 25 auf OCCB1)	81 (6 auf OCCL + 75 auf OCCB3)	–
T.38-Kanäle (Anzahl der gleichzeitig zu sendenden und zu empfangenen T.38-Faxe)	3 auf OCCS	3 auf OCCMR/ OCCM 6 auf OCCMR/ OCCM + OCCB1 12 auf OCCMR/ OCCM + OCCB3	3 auf OCCMR/ OCCM 6 auf OCCMR/ OCCM + OCCB1 12 auf OCCMR/ OCCM + OCCB3	3 auf OCCMR/ OCCM 6 auf OCCMR/ OCCM + OCCB1 12 auf OCCMR/ OCCM + OCCB3	T.38-Fax-Kanäle über Gateway
MEB (Media Extension Bridge)-Kanäle	30	30	30	30	30
Music On Hold MOH					

Ressource		Maximalwerte				
		OpenScape Business				
		X1	X3R X3W	X5R X5W	X8	S
	MOH-Kanäle (G.711, G.729)	0 bis 4 (konfigurationsabhängig)	0 bis 4 (konfigurationsabhängig)	0 bis 4 (konfigurationsabhängig)	0 bis 4 (konfigurationsabhängig)	32 (über Media Server)
	PPP-Kanäle	8	8	8	8	–
DTMF						
	DTMF-Empfänger	16	16	16	16	–

26.2 Software-Kapazitäten

Bei den hier beschriebenen Maximalwerten handelt es sich um die Software-Kapazitäten von OpenScape Business.

Tabelle: Themenbereich Anbindung an Service-Provider

Themenbereich: Anbindung an Service-Provider		Maximalwerte						
		OpenScape Business					UC Booster	
		X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
ITSP (Internet-Telefonie-Service-Provider)-Anbindung:								
	ITSP-Leitungen pro Kommunikationssystem	60	60	60	60	128	–	–
	Gleichzeitig aktivierte ITSPs pro Kommunikationssystem	4	4	4	4	4	–	–
Richtungen:								
	Richtungen pro Kommunikationssystem	16	16	16	16	16	–	–
	Überlaufrichtungen pro Richtung	1	1	1	1	1	–	–

Tabelle: Themenbereich Teilnehmer

Themenbereich: Teilnehmer	Maximalwerte						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
Berechtigungsklassen:							

Themenbereich: Teilnehmer	Maximalwerte						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
Berechtigungsklassen pro Kommunikationssystem	15	15	15	15	15	–	–
Teilnehmerrufnummer/Durchwahlnummer:							
Ziffern pro Teilnehmerrufnummer/Durchwahlnummer	16 (Standardeinstellung = 3)	16 (Standardeinstellung = 3)	16 (Standardeinstellung = 3)	16 (Standardeinstellung = 3)	16 (Standardeinstellung = 3)	–	–

Tabelle: Themenbereich UC Smart

Themenbereich UC Smart	Maximalwerte						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
myPortal Smart	30	50	50	50	–	–	–
Anrufjournal:							
Anrufjournaleinträge pro Benutzer	100	100	100	100	–	–	–
Sprachbox:							
Sprachboxen pro Kommunikationssystem	30	320	320	320	–	–	–
Max. Aufzeichnungsdauer pro Anruf	2 Minuten	2 Minuten	2 Minuten	2 Minuten	–	–	–
Gesamtaufzeichnungsdauer pro Kommunikationssystem	32 Stunden	32 Stunden	32 Stunden	32 Stunden	–	–	–
Nachrichten pro Sprachbox	100	100	100	100	–	–	–
Gleichzeitige Anrufe (kommend und gehend)	10	10	10	10	–	–	–
Anwesenheitsstatus:							
Status pro UC Smart Teilnehmer	9	9	9	9	–	–	–
Sprachbox-Ansagen pro Anwesenheitsstatus	1	1	1	1	–	–	–
AutoAttendant:							
Company AutoAttendant	1	1	1	1	–	–	–

Tabelle: Themenbereich UC Suite

Themenbereich: UC Suite	Maximalwerte						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
myAttendant	–	–	–	–	20 (lizenzabhängig)	20 (lizenzabhängig)	20 (lizenzabhängig)
myPortal for Desktop	–	–	–	–	500 (lizenzabhängig)	500 (lizenzabhängig)	150 (lizenzabhängig)
myPortal for Outlook	–	–	–	–	500 (lizenzabhängig)	500 (lizenzabhängig)	150 (lizenzabhängig)
Anrufjournal (myPortal for Desktop und myPortal for Outlook):							
Archivierungsdauer in den UC Clients	–	–	–	–	30 Tage (Standardeinstellung = 30 Tage)		
Archivierungsdauer im Kommunikationssystem	–	–	–	–	365 Tage (Standardeinstellung = 30 Tage)		
Anrufjournaleinträge	–	–	–	–	Keine Begrenzung		
Aufzeichnen von Anrufen/Konferenzen:[1]							
Aufzeichnungsdauer pro Anruf/Konferenz	–	–	–	–	Wird durch die Länge des Anrufs/der Konferenz begrenzt		
Applikationsgesteuerte Konferenzen:							
Gleichzeitige UC-Konferenzen pro Kommunikationssystem	–	–	–	–	5	5	5
Teilnehmer pro Konferenz	–	–	–	–	16	16	16
Externe Teilnehmer pro Konferenz	–	–	–	–	15	15	15
Konferenzkanäle	–	–	–	–	20 für Meet-Me 20 für Ad Hoc	20 für Meet-Me und Ad Hoc	20 für Meet-Me und Ad Hoc
Externe Datenbankanbindung (LDAP, SQL usw.):							
Externe Datenbankanbindungen pro Kommunikationssystem	–	–	–	–	10	10	10
LDAP-Anbindung der Systemtelefone	siehe Bedienungsanleitung der Systemtelefone					–	–
LDAP-Nutzung über UC Clients (myAttendant, myPortal for Desktop usw.)	–	–	–	–	Jeder Client kann die zentrale LDAP-Anbindung des Kommunikationssystems nutzen		
SQL-Nutzung über UC Clients (myAttendant, myPortal for Desktop usw.)	–	–	–	–	Jeder Client kann die zentrale SQL-Anbindung des Kommunikationssystems nutzen		

Themenbereich: UC Suite	Maximalwerte						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
Sprachbox:[1]							
Sprachboxen pro Kommunikationssystem	–	–	–	–	Für jeden UC Suite Benutzer verfügbar		
Aufzeichnungsdauer	–	–	–	–	15 Minuten pro Anruf (1 Minute Sprache entspricht ca. 1 MB Speicherbedarf)		
Aufzeichnungsdauer, bis zu der eine Weiterleitung von Sprachnachrichten per E-Mail möglich ist	–	–	–	–	Ca. 10 Minuten		
Gleichzeitige Anrufe (kommend und gehend)	–	–	–	–	30	30	30
Faxbox:[1]							
Faxboxen pro Kommunikationssystem	–	–	–	–	200	500	500
Faxlänge in Seiten	–	–	–	–	500 (1 Normfax (2 DIN A4 Seiten) entspricht ca. 48 kB Speicherbedarf)		
Gleichzeitig zu sendende und zu empfangene Faxe	–	–	–	–	8	8	8
Serienfax-Empfänger	–	–	–	–	Keine Begrenzung		
Faxbox-Gruppen pro Kommunikationssystem	–	–	–	–	60	60	60
Teilnehmer pro Faxbox-Gruppe	–	–	–	–	10	10	10
Ansagen:[1]							
Ansagen pro UC Suite Teilnehmer	–	–	–	–	1 Begrüßungsansage, 1 Namensansage, 1 anwesenheitsstatus-bezogene Ansage und 1 Ansage für den persönlichen AutoAttendant		
Anwesenheitsstatus:							
Status pro UC Suite Teilnehmer	–	–	–	–	9	9	9
Sprachbox-Ansagen pro Anwesenheitsstatus	–	–	–	–	1	1	1
Multi-User Chat:							
Interne Kommunikationspartner	–	–	–	–	Keine Begrenzung		
Externe XMPP-Kommunikationspartner	–	–	–	–	1	1	1

Themenbereich: UC Suite	Maximalwerte						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
AutoAttendant:							
Persönlicher AutoAttendant	–	–	–	–	20	20	20
Company AutoAttendant	–	–	–	–	1	1	1

1 Die Gesamtaufzeichnungsdauer für Sprachansagen, Sprachnachrichten, Sprachaufzeichnungen und Faxe ist abhängig von der Festplatte im Kommunikationssystem. Eine Begrenzung für einzelne Teilnehmer gibt es nicht.
Beispiel für eine 160 GB Festplatte: Das Speichervolumen der Partition für die Aufzeichnung von Sprachansagen, Sprachnachrichten, Sprachaufzeichnungen und Faxe beträgt 20 GB. Das entspricht einer Gesamtaufzeichnungsdauer von ca. 20000 Minuten.

Tabelle: Themenbereich Funktionen am Telefon

Themenbereich: Funktionen am Telefon	Maximalwerte						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
Anruferliste:							
Anruferlisten pro Kommunikationssystem	650	650	650	650	650	–	–
Einträge pro Anruferliste	10	10	10	10	10	–	–
Gespeicherte Ziffern pro Eintrag	25stellige Rufnummer und Richtungskennzahl					–	–
Direktruftasten (DSS-Tasten):							
Beistellgeräte pro Kommunikationssystem	30	250	250	250	250	–	–
Beistellgeräte pro Telefon	2	2	2	2	2	–	–
Tasten pro Beistellgerät	12 bei OpenStage Key Module 18 bei OpenStage Key Module 15					–	–
Besetztlampenfelder (BLF) pro Kommunikationssystem	12	12	12	12	12	–	–
Tasten pro Besetztlampenfeld	90	90	90	90	90	–	–
Kurzwahl individuell (KWI):							
Einträge im KWI-Pool pro Kommunikationssystem	2000	2000	2000	2000	2000	–	–
Einträge pro Teilnehmer	10	10	10	10	10	–	–
Ziffern pro Eintrag	25stellige Rufnummer und Richtungskennzahl					–	–
Kurzwahl zentral (KWZ):							
Einträge pro Kommunikationssystem	8000	8000	8000	8000	8000	–	–
Zeichenlänge des Namens	16	16	16	16	16	–	–
Ziffern pro Eintrag	25stellige Rufnummer und Richtungskennzahl					–	–
Wahlwiederholung:							

Themenbereich: Funktionen am Telefon	Maximalwerte						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
Einträge pro Telefon mit Display	3 für optiPoint 410/420 und OpenStage 20E/20/20G/40/40G 10 für OpenStage 15 In OpenStage 60/60G/80/80G können max. 30 Einträge je Rufliste "Angenommen", "Entgangen" und "Gewählt" genutzt werden					–	–
Einträge pro Telefon ohne Display	1	1	1	1	1	–	–
Gespeicherte Ziffern pro Eintrag	25stellige Rufnummer und Richtungskennzahl					–	–
Anklopfen/Rufeinblendung:							
Wartende Anrufer pro Telefon	16	16	16	16	16	–	–
Parken:							
Parkpositionen pro Kommunikationssystem	10	10	10	10	10	–	–
Rückrufe:							
Rückrufeinträge pro Telefon	5	5	5	5	5	–	
Abwesenheitstexte/Mitteilungstexte:							
Abwesenheitstexte pro Kommunikationssystem	250	250	250	250	250	–	–
Mitteilungstexte pro Kommunikationssystem	150	150	150	150	150	–	–
Konfigurierbare Abwesenheitstexte + Mitteilungstexte pro Kommunikationssystem	10 + 10	10 + 10	10 + 10	10 + 10	10 + 10	–	–
Zeichenlänge eines konfigurierbaren Abwesenheitstextes/Mitteilungstextes	24	24	24	24	24	–	–
Empfangene Abwesenheitstexte/Mitteilungstexte pro Telefon mit Display	5	5	5	5	5	–	–
Empfangene Abwesenheitstexte/Mitteilungstexte pro Telefon ohne Display	1	1	1	1	1	–	–
Rufzuschaltung:							
Zugeschaltete Teilnehmer	5	5	5	5	5	–	–
Anrufumleitung (AUL):							
AUL-Ziele pro Telefon	4	4	4	4	4	–	–
Ziffern pro externem AUL-Ziel	25stellige Rufnummer und Richtungskennzahl					–	–
Verkettete AUL-Ziele					5	–	
Systemgesteuerte Konferenzen:							

Themenbereich: Funktionen am Telefon	Maximalwerte						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
Gleichzeitige System-Konferenzen pro Kommunikationssystem	6	6	6	6	6	–	–
Teilnehmer pro Konferenz	8	8	8	8	8	–	–
Externe Teilnehmer pro Konferenz	7	7	7	7	7	–	–
Konferenzkanäle	32	32	32	32	20	–	–
Türsprechstelle, Türöffner:							
Anschlüsse über a/b-Schnittstellen pro Kommunikationssystem	4	4	4	4	–	–	–
Ziffern pro Codeeintrag	5	5	5	5	–	–	–
Leitungsvormerken:							
Gleichzeitige Einträge pro Kommunikationssystem	32	32	32	32	–	–	–

Tabelle: Themenbereich Arbeiten im Team (Gruppen)

Themenbereich: Arbeiten im Team (Gruppen)	Maximalwerte						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
Anrufübernahmegruppen:							
Anrufübernahmegruppen pro Kommunikationssystem	32	32	32	32	32	–	–
Teilnehmer pro Anrufübernahmegruppe	32	32	32	32	32	–	–
Gruppenrufe, Sammelanschlüsse, Basic-MULAPs, Chef-MULAPs, Team-Gruppen, Top-Gruppen, Sprachbox-Gruppen:							
Summe der Gruppenrufe, Sammelanschlüsse, Basic-MULAPs, Chef-MULAPs und Sprachbox-Gruppen pro Kommunikationssystem	800	800	800	800	800	–	–
Summe der Team-Gruppen und Top-Gruppen pro Kommunikationssystem	500	500	500	500	500	–	–
Teilnehmer pro Gruppenruf, Sammelanschluss, Basic-MULAP	20	20	20	20	20	–	–
Teilnehmer pro Chef-MULAP, Team-Gruppe, Top-Gruppe	10	10	10	10	10	–	–
Teilnehmer pro Sprachbox-Gruppe	20	20	20	20	20	–	–
MULAP-Tasten pro Telefon	10	10	10	10	10	–	–
Faxbox-Gruppen:							

Themenbereich: Arbeiten im Team (Gruppen)	Maximalwerte						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
Faxbox-Gruppen pro Kommunikationssystem: Siehe Tabelle: Themenbereich UC Suite							
Durchsage an Gruppe:							
Gleichzeitige Durchsagen pro Kommunikationssystem	1	1	1	1	6	–	–
Empfänger der Durchsage	20	20	20	20	20	–	–
UCD-Gruppen:							
UCD-Gruppen pro Kommunikationssystem	60	60	60	60	60	–	–
Ansagen pro UCD-Gruppe	7	7	7	7	7	–	–
Prioritätsebenen pro UCD-Gruppe	10	10	10	10	10	–	–
Wartende Anrufe pro UCD-Gruppe	30	30	30	30	30	–	–
UCD-Agenten:							
UCD-Agenten-IDs pro Kommunikationssystem	330	330	330	330	330	–	–
Gleichzeitig aktive UCD-Agenten pro Kommunikationssystem	64	64	64	64	64	–	–
Ansagen bei UCD:							
Anrufer pro Kommunikationssystem, denen gleichzeitig eine Ansage eingespielt werden kann	8	8	8	8	8	–	–

Tabelle: Themenbereich Anruf-Routing

Themenbereich: Anruf-Routing	Maximalwerte						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
Amtsberechtigung:							
Erlaubnislisten	6	6	6	6	6	–	–
Verbotslisten	6	6	6	6	6	–	–
Erlaubnisliste kurz (10 Einträge)	5	5	5	5	5	–	–
Erlaubnisliste lang (100 Einträge)	1	1	1	1	1	–	–
Verbotsliste kurz (10 Einträge)	5	5	5	5	5	–	–
Verbotsliste lang (50 Einträge)	1	1	1	1	1	–	–
Zeichenlänge der Listeneinträge	32	32	32	32	25	–	–
Leitweglenkung (LCR):							

Themenbereich: Anruf-Routing	Maximalwerte						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
Gewählte/geprüfte Ziffern	24	24	24	24	24	–	–
Wahlpläne	1000	1000	1000	1000	1000	–	–
Wegetabellen	254	254	254	254	254	–	–
Wege pro Wegetabelle	16	16	16	16	16	–	–
Wahlregeln pro Richtung	254	254	254	254	254	–	–
Ziffern pro Wahlregel	40	40	40	40	40	–	–
Nachtschaltung:							
Berechtigte Teilnehmer pro Kommunikationssystem	5	5	5	5	5	–	–
Notrufdienst E911 (nur für USA):							
Ziffern pro LIN (Location Identification Number)	16	16	16	16	16	–	–
Röchelschaltung/Hotline:							
Hotlineziele pro Kommunikationssystem	6	6	6	6	6	–	–
VBZ-Gruppen:							
VBZ-Gruppen pro Kommunikationssystem	64	64	64	64	64	–	–

Tabelle: Themenbereich Attendants

Themenbereich: Attendants	Maximalwerte						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
myAttendant: Siehe Tabelle: Themenbereich UC Suite							
AutoAttendant (UC Smart): Siehe Tabelle: Themenbereich UC Smart							
AutoAttendant (UC Suite): Siehe Tabelle: Themenbereich UC Suite							
AutoAttendant (Xpressions Compact):							
Persönlicher AutoAttendant	–	30 mit IVMP4R / 100 mit IVMS8NR 30 mit IVMP4 / 100 mit IVMS8N		100 mit IVMNL	–	–	–
OpenScape Business Attendant:							
OpenScape Business Attendants pro Kommunikationssystem	8	8	8	8	8	–	–

Tabelle: Themenbereich Multimedia Contact Center

Themenbereich: Multimedia Contact Center	Maximalwerte						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
myAgent:							
Lizenzierbare Agenten	–	–	–	–	192	192	192
Gleichzeitig aktive Agenten	–	–	–	–	64	64	64
myReports	–	–	–	–	1	1	1
Warteschlangen:							
Warteschlangen pro Kommunikationssystem	–	–	–	–	50	50	50
Nachbearbeitung:							
Nachbearbeitungs-Codes pro Warteschlange	–	–	–	–	Keine Begrenzung	Keine Begrenzung	Keine Begrenzung

Tabelle: Themenbereich Mobility

Themenbereich: Mobility	Maximalwerte						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
Teleworker-Arbeitsplätze:							
Teleworker-Arbeitsplätze über VPN pro Kommunikationssystem	10	10	10	10	Möglich über externen Router	–	–
Mobility Teilnehmer:							

Themenbereich: Mobility	Maximalwerte						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
Mobility: Teilnehmer pro Kommunikationssystem	30	150	150	150	–	–	–
myPortal for Mobile/Tablet (UC Smart): Teilnehmer pro Kommunikationssystem	30 (konfigurierbar) / 30 (gleichzeitig aktiv)	50 (konfigurierbar) / 30 (gleichzeitig aktiv)	50 (konfigurierbar) / 30 (gleichzeitig aktiv)	50 (konfigurierbar) / 30 (gleichzeitig aktiv)	–	–	–
myPortal for Mobile/Tablet (UC Suite): Teilnehmer pro Kommunikationssystem	–	–	–	–	200 (konfigurierbar) / 30 (gleichzeitig aktiv)	100 (konfigurierbar) / 30 (gleichzeitig aktiv)	100 (konfigurierbar) / 30 (gleichzeitig aktiv)
myPortal to go (UC Smart): Teilnehmer pro Kommunikationssystem	30	50	50	50	–	–	–
myPortal to go (UC Suite): Teilnehmer pro Kommunikationssystem	–	–	–	–	200 (konfigurierbar) / 100 (gleichzeitig aktiv)	100	100

Tabelle: Themenbereich Security

Themenbereich: Security	Maximalwerte						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
VPN:							
VPN-Tunnel	256	256	256	256	Möglich über externen VPN-Router	–	–
VPN-Regeln	634	634	634	634		–	–
Individuelles Codeschloss:							
Ziffern pro Telefonschlosscode	5	5	5	5	5	–	–
Zulässige Zeichen	0 bis 9	0 bis 9	0 bis 9	0 bis 9	0 bis 9	–	–

Tabelle: Themenbereich Vernetzung von OpenScape Business

Themenbereich: Vernetzung von OpenScape Business[1]	Maximalwerte
Vernetzung von OpenScape Business X3R/X3W, OpenScape Business X5R/X5W, OpenScape Business X8, OpenScape Business S und OpenScape Business UC Booster Server:	
Vernetzte Kommunikationssysteme (Knoten)	8 (mit UC Suite) / 32 (ohne UC Suite)
Teilnehmer im Netz	1000

1 Darüber hinausgehende Ausbaugrenzen für Vernetzungen können über projektspezifische Freigaben beantragt werden. Bitte beachten Sie die aktuelle Vertriebsfreigabe.

Tabelle: Themenbereich Anschaltungen

Themenbereich: Anschaltungen	Maximalwerte						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
OpenStage Gate View:							
Kameras pro Kommunikationssystem	–	–	–	–	8 (lizenzabhängig)	8 (lizenzabhängig)	2 (lizenzabhängig)
Telefone (OpenStage HFA 60, 60 G, 80, 80 G, 80 E) für die Darstellung des Kamerabilds pro Kommunikationssystem	–	10 (mit OCAB) 20 (mit Application Server)			20	–	–
iPhone Apps oder Web-Clients für die Darstellung des Kamerabilds pro Kommunikationssystem	–	10 (mit OCAB) 20 (mit Application Server)			20	–	–

Tabelle: Themenbereich Application Connectivity

Themenbereich: Application Connectivity	Maximalwerte						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
CSTA:							
CSTA-Links via CSP pro Kommunikationssystem	–	–	–	–	4	4	4
Monitorpunkte für Amtsleitungen oder Teilnehmer	–	–	–	–	700	700	700
TAPI 170 Middleware Server	–	–	–	–	1	1	1
Web Services Interface Protocol:							
Web Server WebSessions	100	100	100	100	200	100	100
Interne Monitorpunkte	800	800	800	800	800	800	800

Tabelle: Themenbereich Accounting

Themenbereich: Accounting	Maximalwerte						
	OpenScape Business					UC Booster	
	X1	X3R X3W	X5R X5W	X8	S	UC Booster Server	UC Booster Card
Gesprächsdatenerfassung zentral:							
Einträge im Gesprächsdatenpuffer pro Kommunikationssystem	20000	20000	20000	20000	20000	–	–
Projektkennzahl (PKZ):							
PKZ-Einträge pro Kommunikationssystem	1000	1000	1000	1000	1000	–	–
Prüfbare Ziffern pro PKZ	11	11	11	11	11	–	–
Zulässige Zeichen	0 bis 9	0 bis 9	0 bis 9	0 bis 9	0 bis 9	–	–

27 Experten-Modus

Der **Experten-Modus** stellt Menüs mit Funktionen für die Konfiguration und Wartung des Systems zur Verfügung.

27.1 Darstellungskonventionen für Parameterbeschreibungen

Die Parameterbeschreibungen folgen der Struktur des Experten-Modus im WBM.

Menüeintrag	Jedem Menüeintrag des Experten-Modus ist ein Hilfe-Topic zugeordnet, das Sie direkt (kontext-sensitiv) aus dem WBM aufrufen können. Die Überschrift des Hilfe-Topics zeigt den Pfad des WBM-Fensters. Beispiel: **Grundeinstellungen > System > System Flags**
Registerkarte	Jeder Registerkarte ist eine eigene Parameter-Tabelle im Hilfe-Topic zugeordnet. Gleiche Parameter unterschiedlicher Registerkarten werden in der selben Parameter-Tabelle beschrieben. Über jeder Parameter-Tabelle finden Sie eine Auflistung für welche Registerkarte(n) die Parameter gelten. Beispiel: • **Statische IP Adresse hinzufügen** • **Statische IP Adresse ändern** • **Statische IP Adresse löschen**
Bereich	Wenn WBM-Fenster in Bereiche strukturiert sind, finden Sie diese Struktur auch in der Parameter-Tabelle wieder. Die Parameter-Tabelle enthält dann für jeden Bereich eine Zwischenüberschrift, gefolgt von den Parametern dieses Bereichs.
Parameter	Parameter werden in einer zweispaltigen Parameter-Tabelle beschrieben. Die linke Spalte nennt Parameter. Die rechte Spalte beschreibt Parameter. Selbsterklärende Parameter werden genannt aber nicht beschrieben. Wertebereich und Standardwert (Default) finden Sie am Ende der Beschreibung, sofern vorhanden.

Parameter (optional)	Parameter, die nicht ausgefüllt werden müssen, sind mit dem Schlüsselwort optional gekennzeichnet.
Eintrag in Aufklappliste	Nicht selbsterklärende Einträge in Aufklapplisten werden auch als Parameter in der linken Spalte der Parameter-Tabelle genannt. Der Eintrag wird durch einen Doppelpunkt vom Namen der Aufklappliste getrennt. Beispiel: **Verschlüsselungsalgorithmen: AES**
Kontrollkästchen/Optionsfeld/Flag	Die Beschreibung von Kontrollkästchen/Optionsfeldern/Flags bezieht sich immer auf den aktivierten Zustand.

27.2 Wartung

Unter **Wartung** sind Funktionen für die Wartung des Kommunikationssystems zusammengefasst, um z. B. Wartemusik einzuspielen oder die Software-Images zu aktualisieren.

27.2.1 Konfiguration

Unter **Konfiguration** sind Funktionen zusammengefasst, um z. B. Wartemusik (MoH) zu laden oder die Hardware-Konfiguration anzuzeigen.

27.2.1.1 Konfiguration > Wartemusik (MoH) > Laden zum Gateway

Parameterbeschreibung der Registerkarten:

- **Wartemusik-Dateien über HTTP hochladen**

Parameter	Beschreibung
Wartemusik-Dateien über HTTP hochladen	
Wartemusik-Datei - Tag	Auswählen der MoH-Datei für Tag vom lokalen Dateisystem. Dateiformat: siehe Hinweis im WBM.
Wartemusik-Datei - Nacht	Auswählen der MoH-Datei für Nacht vom lokalen Dateisystem. Dateiformat: siehe Hinweis im WBM.
Laden	Hochladen der gewählten MoH-Dateien in das System (erfordert Neustart). Aktivierung unter Einrichtung, Zentrale Telefonie > Wartemusik/Ansagen.

Parameterbeschreibung der Registerkarten:

- **Audiodateien über HTTP hochladen**

Parameter	Beschreibung
Audiodateien über HTTP hochladen	
Ansagedatei	Auswählen der WAV-Datei mit der Ansage vom lokalen Dateisystem auswählen. Dateiformat: siehe Hinweis im WBM.
Bereits hochgeladene Audiodateien	
WAV-Datei	Anzeige der im Kommunikationssystem geladenen Ansagedateien
Löschen	Löschen der Ansagedatei
Laden	Hochladen der gewählten Ansagedatei in das System. Aktivierung unter Einrichtung, Zentrale Telefonie > Wartemusik/Ansagen.

27.2.1.2 Konfiguration > Ansagen > Laden zum Gateway

Parameterbeschreibung der Registerkarten:

- **Audiodateien über HTTP hochladen**

Parameter	Beschreibung
Audiodateien über HTTP hochladen	
Ansagedatei	Auswählen der WAV-Datei mit der Ansage vom lokalen Dateisystem auswählen. Dateiformat: siehe Hinweis im WBM.
Bereits hochgeladene Audiodateien	
WAV-Datei	Anzeige der im Kommunikationssystem geladenen Ansagedateien
Löschen	Löschen der Ansagedatei
Laden	Hochladen der gewählten Ansagedatei in das System. Aktivierung unter Einrichtung, Zentrale Telefonie > Wartemusik/Ansagen.

27.2.1.3 Konfiguration > Port-Konfiguration

Parameterbeschreibung der Registerkarte:

- **Konfiguration exportieren**

Parameter	Beschreibung
Konfiguration exportieren	
Dateiname	Name der exportierten Datei.
Aktion	Export einer gezippten XML-Datei (z. B. für Bearbeitung in Excel) mit folgenden Daten: Name, Rufnummer des Teilnehmers, Durchwahlnummer, Stationstyp, Lizenzen, Gruppen, virtuelle Teilnehmer, Leitungen, Leitungsgruppen, Voicemail usw.

27.2.1.4 Konfiguration > SmartVM

Parameterbeschreibung der Registerkarten:

- **Übersicht**

Parameter	Beschreibung
Sprachen Anzeige aller Sprachen, in denen die Sprachbenutzerführung vorliegt. Es gilt die folgende Namenskonvention: aabb aa = zweistelliger Sprachcode bb = zweistelliger Ländercode Der Ländercode (bb) ist in der Regel mit dem Sprachcode (aa) identisch	
Mailbox-Informationen	
Rufnummer	Anzeige der Mailbox-Rufnummer.
Name	Anzeige des Mailbox-Namens.
Nachrichten	Anzeige der Anzahl neuer Nachrichten / Anzahl aller Nachrichten.
Mailbox-Belegung gesamt	Anzeige des Speicherplatzverbrauchs in Prozent.

27.2.1.5 Konfiguration > SmartVM > Mailbox-Operationen

Parameterbeschreibung der Registerkarten:

- **Mailbox-Operationen ausführen**

Parameter	Beschreibung
Alle Mailbox-Konfigurationen zurücksetzen (alle Nachrichten und Begrüßungsansagen löschen)	Ist dieses Flag aktiviert, werden alle Begrüßungen und Nachrichten aller Sprachboxen auf SmartVM gelöscht. Standard: Deaktiviert.
Index	Anzeige des Index der Sprachbox.
Rufnr.	Anzeige der Sprachbox-Rufnummer.

Parameter	Beschreibung
Name	Anzeige des Namens der Sprachbox.
Passwörter zurücksetzen	Ist dieses Flag aktiviert, wird das Kennwort der Sprachbox auf das Standardkennwort `123456` zurückgesetzt. Der Benutzer muss das Kennwort bei der nächsten Benutzung der Sprachbox ändern. Standard: Deaktiviert.
Mailboxen initialisieren	Ist dieses Flag aktiviert, werden für die ausgewählte Sprachbox folgende Aktionen ausgeführt: Standard Mailboxen: – Passwort wird zurückgesetzt – Flag **Aufnahme** wird gesetzt – Nachrichten werden gelöscht – Begrüßungen werden gelöscht – Begrüßungskontrolle auf manuell – Aktive Begrüßung: Begrüßung 1 AutoAttendant Mailboxen: – Passwort wird zurückgesetzt – Flag **Abwurf nach Ansage** wird deaktiviert – Kurzwahlziele werden gelöscht – Begrüßungen werden gelöscht – Begrüßungskontrolle auf manuell – Aktive Begrüßung: Begrüßung 1 Standard: Deaktiviert.

27.2.1.6 Konfiguration > SmartVM > Dateioperationen

Parameterbeschreibung der Registerkarten:

- **Backup**

Parameter	Beschreibung
Backup	
Messages	Ist diese Flag aktiviert, werden zusätzlich zu den Begrüßungen auch die Nachrichten der ausgewählten Sprachboxen gesichert. Standard: Deaktiviert.
Verfügbare Mailboxen	Liste aller vorhandenen Sprachboxen. Es können einzelne oder auch alle Sprachboxen in die Liste der zu sichernden Sprachboxen aufgenommen werden.

Parameter	Beschreibung
Zu sichernde Mailboxen	Liste der zu sichernden Sprachboxen.
Schaltflächen	
Übernehmen	Die Begrüßungen (und die Nachrichten, wenn Flag **Messages** aktiviert) der zu sichernden Sprachboxen werden in eine Sicherungsdatei (`*.tar`) gesichert.

Parameterbeschreibung der Registerkarten:

- **Begrüßungsansagen**

Parameter	Beschreibung
Begrüßungsansagen	
Mailbox-Auswahl	Auswahl der Sprachbox.
Begrüßung 1 (Tag)	Anzeige der momentan verwendeten Begrüßung. **Standard** bedeutet: es ist keine individuelle Begrüßung für den Teilnehmer vorhanden.
Begrüßung 2 (Nacht)	Anzeige der momentan verwendeten Begrüßung. **Standard** bedeutet: es ist keine individuelle Begrüßung für den Teilnehmer vorhanden.
Begrüßung 3	Anzeige der momentan verwendeten Begrüßung. **Standard** bedeutet: es ist keine individuelle Begrüßung für den Teilnehmer vorhanden.
Begrüßung 4	Anzeige der momentan verwendeten Begrüßung. **Standard** bedeutet: es ist keine individuelle Begrüßung für den Teilnehmer vorhanden.
Schaltflächen	
Durchsuchen	Navigation zum Ablagepfad der Begrüßungsdatei.
Laden	Eine zuvor gespeicherte Begrüßung oder eine Wave-Datei wird in die SmartVM geladen. Die zu ladende Wave-Datei muss folgendes Format haben: PCM, 16 bit, 8khz, mono Beim Laden wird die ausgewählte Wave-Datei konvertiert. Je nach Größe der Wave-Datei kann dies einige Zeit in Anspruch nehmen.
Sichern	Die momentan verwendete Begrüßung wird auf den PC gesichert. Die Begrüßung wird im Binär-Format auf dem PC gespeichert (vma-Datei) und kann deshalb nicht abgespielt oder geändert werden.
Löschen	Die momentan verwendete Begrüßung wird aus der SmartVM gelöscht.

Parameterbeschreibung der Registerkarten:

- **Restore**

Parameter	Beschreibung
Restore	
Nachrichten	Überschreibt nicht nur die Begrüßungen der ausgewählten Sprachboxen, sondern auch die Nachrichten. Standard: Deaktiviert.
Aufschalten	Ist dieses Flag deaktiviert, werden nur die Begrüßungen der ausgewählten Sprachboxen überschrieben, die in den Sicherungsdaten vorhandenen sind. Ist zusätzlich das Flag **Nachrichten** aktiviert, werden auch die in den Sicherungsdaten enthaltenen Nachrichten hinzugefügt. Die bereits existierenden Nachrichten bleiben erhalten. Ist dieses Flag aktiviert, werden vor der Wiederherstellung alle Begrüßungen und Nachrichten der ausgewählten Sprachboxen in der SmartVM gelöscht. Sind Sprachboxen ausgewählt, die nicht in den Sicherungsdaten enthaltenen sind, werden diese auch gelöscht! Die in den Sicherungsdaten enthaltenen Begrüßungen werden übertragen. Ist zusätzlich das Flag **Nachrichten** aktiviert, werden auch die in den Sicherungsdaten enthaltenen Nachrichten übertragen. Standard: Deaktiviert.
Verfügbare Mailboxen	Liste aller in der Sicherungsdatei vorhandenen Sprachboxen. Es können einzelne oder auch alle Sprachboxen in die Liste der wiederherzustellenden Sprachboxen aufgenommen werden.
Zu sichernde Mailboxen	Liste der zu wiederherzustellenden Sprachboxen.
Schaltflächen	
Durchsuchen	Navigation zum Ablagepfad der Sicherungsdatei.
Laden	Die in der Sicherungsdatei enthaltenen Sprachboxen werden angezeigt. Ein erneutes Anklicken der Schaltfläche stellt die Begrüßungen und Nachrichten der ausgewählten Sprachboxen wieder her.

27.2.1.7 Konfiguration > Branding

Parameterbeschreibung der Registerkarte:

- **Branding**

Parameter	Beschreibung
Branding	Auswahl der Produktbezeichnung.

27.2.1.8 Konfiguration > IP-Gateway-Adresse

Parameterbeschreibung der Registerkarte:

- **IP Gateway-Adresse ändern**

Parameter	Beschreibung
IP-Gateway-Adresse ändern	
Gateway-IP-Adresse	Eingabe der IP-Adresse des Kommunikationssystems, z. B. 192.168.1.2

27.2.2 Software-Image

Unter **Software-Image** sind die Funktionen für das Aktualisieren der Gateway-Software und der Telefon-Images zusammengefasst.

27.2.2.1 Software-Image > System-Software > Update via Internet

Parameterbeschreibung der Registerkarten:

- **Laden der Software-Images von einem Webserver**

Parameter	Beschreibung
Webserver Einstellungen	
Software-Image URL	Anzeige und Änderung des Links zum Software-Server inkl. Pfad zur Image-Datei.
Benutzername	Benutzername für die Anmeldung am Software-Server.
Passwort	Passwort für die Anmeldung am Software-Server.
Software Update-Information	Aktivierung der Abfrage, ob am Software-Server eine neue Software-Version bereitgestellt ist.
Startzeit	Zeitpunkt der Abfrage. Wertebereich: 00.00 - 24.00, Standardwert: 02.00
Proxy verwenden	Proxy-Aktivierung, falls ein Proxy verwendet wird.
HTTP-Proxy	
HTTP-Proxy	Eingabe des Links zum Proxy-Server.
HTTP-Proxy Port	Eingabe des Ports des Proxy-Servers. Standardwert: 80
Benutzername	Benutzername für die Anmeldung am Proxy-Server.
Passwort	Passwort für die Anmeldung am Proxy-Server.
Letzter Software Update	Anzeige, wann das letzte Software-Update durchgeführt wurde.
Schaltflächen	
Voreinstellung	Setzt die geänderten Werte wieder auf die Standardwerte zurück.

27.2.2.2 Software-Image > System-Software > Update via File Upload

Parameterbeschreibung der Registerkarten:

- **Laden der Software-Images über Datei-Upload**

Parameter	Beschreibung
Remote-Dateiname (PC-Dateisystem)	Navigation zum Ablageort der Image-Datei.
Software-Aktivierung	
Start der Aktion Sofort nach der Übertragung	Die Software wird sofort im Hintergrund in das Kommunikationssystem übertragen. Nach zwei Neustarts ist die Software aktualisiert.
Start der Aktion in	Die Software wird sofort im Hintergrund in das Kommunikationssystem übertragen. Nach Ablauf des angegebenen Zeitraums wird die Software aktiviert. Eingabe des Zeitraum in Tagen, Stunden und Minuten.
Start der Aktion am	Die Software wird sofort im Hintergrund in das Kommunikationssystem übertragen. Zu dem angegebenen Zeitpunkt wird die Software aktiviert. Eingabe des Zeitpunkt als Datum und Uhrzeit.
Lokale Systemzeit	Anzeige von Datum und Uhrzeit des Systems.
Softwareversion des aktuell verwendeten System Software-Images	Anzeige der Softwareversion der aktuellen Image-Datei.

27.2.2.3 Software-Image > System-Software > Update via USB Stick

Parameterbeschreibung der Registerkarten:

- **Laden der Software-Images vom USB-Stick**

Parameter	Beschreibung
Liste aller vorhandenen kompatiblen Image-Dateien	
Versionsnummer	Anzeige der Versionsnummer der auf dem USB-Medium gefundenen Image-Dateien.
Laden	Markieren der auf dem USB-Medium gefundenen Image-Datei, die für die Software-Aktualisierung verwendet werden soll.
Dateiname	Anzeige der Dateinamen der auf dem USB-Medium gefundenen Image-Dateien.
Dateigröße (MB)	Anzeige der Dateigröße der auf dem USB-Medium gefundenen Image-Dateien.
Software-Aktivierung	
Start der Aktion Sofort nach der Übertragung	Die Software wird sofort im Hintergrund in das Kommunikationssystem übertragen und aktiviert. Zur Aktivierung erfolgt eine vorübergehende Unterbrechung des Anlagenbetriebs.
Start der Aktion in	Die Software wird sofort im Hintergrund in das Kommunikationssystem übertragen. Nach Ablauf des angegebenen Zeitraums wird die Software aktiviert. Eingabe des Zeitraum in Tagen, Stunden und Minuten.

Parameter	Beschreibung
Start der Aktion am	Die Software wird sofort im Hintergrund in das Kommunikationssystem übertragen. Zu dem angegebenen Zeitpunkt wird die Software aktiviert. Eingabe des Zeitpunkts mit Datum und Uhrzeit.
Lokale Systemzeit	Anzeige von Datum und Uhrzeit des Systems.
Softwareversion des aktuell verwendeten System Software-Images	Anzeige der aktiven Softwareversion.

27.2.2.4 Software-Image > Telefon-Images > Laden

Parameterbeschreibung der Registerkarten:

- **Laden der Telefonsoftware**

Parameter	Beschreibung
Remote-Dateiname (PC-Dateisystem)	Auswahl der Telefonsoftware (Image-Datei)
Aktuell installierte Images	
Löschen	Die Telefon-Images werden zum Löschen markiert.
Dateiname	Anzeige des Dateinamens der Image-Datei.
Gerätetyp	Anzeige des Systemtelefontyps der zur Image-Datei gehört.
Version	Anzeige der Version der Image-Datei.
Schaltflächen	
Laden	Das angegebene Telefon-Image wird in das Kommunikationssystem geladen.
Löschen	Die markierten Telefon-Images werden vom Kommunikationssystem gelöscht.

27.2.2.5 Software-Image > Telefon-Images > Verteilen

Parameterbeschreibung der Registerkarten:

- **Verteilen der Telefonsoftware**

Parameter	Beschreibung
Aktuell installierte Images	
Verteilen	Ist das Kontrollkästchen aktiviert, wird diese Telefonsoftware an alle angeschlossenen Systemtelefone des Telefontyps übertragen.
Dateiname	Anzeige des Dateinamens der Image-Datei.
Gerätetyp	Anzeige des Systemtelefontyps, der zur Image-Datei gehört.

Parameter	Beschreibung
Version	Anzeige der Version der Image-Datei.
Typ	Typ des Systemtelefons.
Standard	Als Standard markierte Telefonsoftware wird automatisch auf ein diesem Typ zugehöriges Systemtelefon übertragen, wenn es sich zum ersten Mal am System anmeldet.

27.2.2.6 Software-Image > Telefon-Images > Verteilen pro Endgerät

Parameterbeschreibung der Registerkarten:

- **Verteilen der Telefonsoftware pro Endgerät**

Parameter	Beschreibung
Aktuell installierte Images	
Rufnr	Rufnummer des Systemtelefons.
Endgeräte Typ	Typ des Systemtelefons.
IP Adresse	IP-Adresse des Systemtelefons; direkter Link zum WBM des Systemtelefons.
MAC Adresse	MAC-Adresse des Systemtelefons.
Aktuelle SW-Version	Aktuelle Software-Version des Systemtelefons.
verteilbare Software	Auswahl des Telefon-Images, das an das Systemtelefon übertragen werden soll.

27.2.2.7 Software-Image > Telefon-Logo-Images > Laden

Ein Bild (z. B. ein Firmen-Logo) kann auf das Display der Systemtelefone (OpenStage 40/60/80 bzw. Telekom-Varianten) geladen werden, Anzeige im Ruhezustand (on-hook). Spezifikation der Logo-Datei siehe *Telefon-Logos*.

Parameterbeschreibung der Registerkarten:

- **Laden des Telefon-Logos**

Parameter	Beschreibung
Remote-Dateiname (PC-Dateisystem)	Auswahl der Datei mit dem Telefon-Logo.
Aktuell installierte Logo-Images	
Löschen	Die Telefon-Logo-Dateien werden zum Löschen markiert.
Dateiname	Anzeige des Dateinamens der Telefon-Logo-Datei.
Schaltflächen	
Laden	Die angegebene Telefon-Logo-Datei wird in das Kommunikationssystem geladen.
Löschen	Die markierten Telefon-Logo-Dateien werden vom Kommunikationssystem gelöscht.

27.2.2.8 Software-Image > Telefon-Logo-Images > Verteilen

Ein Bild (z. B. ein Firmen-Logo) kann auf das Display der Systemtelefone (OpenStage 40/60/80 bzw. Telekom-Varianten) geladen werden, Anzeige im Ruhezustand (on-hook). Spezifikation der Logo-Datei siehe *Telefon-Logos*.

Parameterbeschreibung der Registerkarten:

- **Verteilen des Telefon-Logos**

Parameter	Beschreibung
Aktuell installierte Logo-Images	
Verteilen	Ist das Kontrollkästchen aktiviert, wird diese Telefon-Logo-Datei an die ausgewählten Systemtelefone übertragen.
Dateiname	Anzeige des Dateinamens der Telefon-Logo-Datei.
An Workpoints folgenden Typs verteilen	Auswahl, ob das Telefon-Logo an alle Systemtelefone oder nur an einen bestimmten Systemtelefontyp übertragen werden soll.

27.2.3 Cordless

Unter **Cordless** sind die Funktionen für alle konfigurierten Basisstationen zusammengefasst.

27.2.3.1 Cordless > Basisstationen

Parameterbeschreibung der Registerkarten:

- **Basisstation Status**

Parameter	Beschreibung
Base Station Daten	
BS Frequenz	Zeigt die Frequenzen der ausgewählten Basistation an. Es können bis zu 10 verschiedene Frequenzkanäle gleichzeitig ausgewählt werden (siehe nachfolgende Tabelle).
Basestation	Nummer der Basisstation.
SW-Version	Software-Version der Basisstation.
HW-Version	Hardware-Version der Basisstation.

Parameter	Beschreibung
Status	Zustand des zugehörigen Ports: Port aktiv Port nicht angeschlossen Port gesperrt Port angeschlossen, nicht aktiv Port angeschlossen, nicht aktiv 1. Zusatzport zu ... (Nr. des Mutterports) 2. Zusatzport zu ... (Nr. des Mutterports)
Overload	Anzahl der Overload-Situationen an der UP0/E -Schnittstelle.
Restart	Anzahl der Restarts der Basisstation.
L1/L2 Error	Anzahl der an der Basisstation aufgetretenen L1/L2-Fehler.
Abnormal Release	Anzahl der abgebrochenen Gespräche der Basisstation.
Calls per BS	Anzahl der Gespräche über die Basisstation (kommend und gehend gemeinsam).
Hopping Mode	Cordless Version 2 Systeme arbeiten immer im ”Fast Hopping Mode”, d.h. es können alle Frequenz-Zeitschlitzpaare benutzt werden. Es stehen also 120 Duplexkanäle zur Verfügung. Bei Slow Hopping BS kann nur jedes zweite Frequenz-Zeitschlitzpaar benutzt werden. Es stehen also nur 60 Duplexkanäle zur Verfügung. Alle Cordless Version 1 Systeme arbeiten im ”Slow Hopping Mode”.
BHO Count OK	Anzahl der erfolgreich durchgeführten Intracell Handovers (Bearer Handovers BHO), d.h. erfolgreiche Wechsel der Trägerfrequenz und/oder des Zeitschlitzes innerhalb einer Funkzelle. Nicht unterstützt durch Hicom cordless EM V2.1 und V2.2. Der Zähler wird zwar nicht unterstützt, aber das Leistungsmerkmal des Bearer Handover steht zur Verfügung.
BHO Count not OK	Anzahl der nicht erfolgreich durchgeführten Intracell Handovers (Bearer Handovers BHO). Nicht unterstützt durch Hicom cordless EM V2.1 und V2.2. Der Zähler wird zwar nicht unterstützt, aber das Leistungsmerkmal des Bearer Handover steht zur Verfügung.
Intra SLC Handover	Anzahl der Handover-Vorgänge innerhalb der Baugruppe SLC16. Gezählt wird bei der neuen Basisstation.
Inter SLC Handover	Anzahl der Handover-Vorgänge zwischen SLC16-Baugruppen. Gezählt wird bei der neuen Basisstation.
SLC16-wide	
Lost Calls	Anzahl von Gesprächen, die aus Ressourcengründen nicht vermittelt werden konnten.
SLMC Overload	Anzahl der Overload-Situationen auf der Baugruppe SLC16. Die Anzahl der freien Poolelemente auf der SLC16-Baugruppe unterschreitet einen Minimalwert. Alle kommenden Belegungen werden von der IWU der SLC16 abgewiesen, bis die Überlastsituation beendet ist.
LR Roam	LR Roam zählt jede Belegung eines Mobiltelefons mit einem Standard-PMID und geänderter Aufenthalts-SLC. Es handelt sich um die Anzahl der Locate-Request-Nachrichten, die Roaming berichteten (d.h. der aktuelle Aufenthaltsort des Mobiltelefons ist verändert). Das Mobiltelefon führt mit jedem Einschalten ein Locate Request durch. Wird das Mobiltelefon ausgeschaltet und in einer anderen Funkzelle eingeschaltet, zählt dieser Zähler nicht.

Parameter	Beschreibung
LR Async	LR Async zählt jede Belegung eines Mobiltelefons mit einem Standard- PMID bei gleichbleibender Aufenthalts-SLC. Es handelt sich um die Anzahl der Locate-Request-Nachrichten, die Asynchronität von Layern berichteten (d.h. der aktuelle Aufenthaltsort des Mobiltelefons ist unverändert). Die Zählung erfolgt jedoch immer auf der Heimat-SLC und zählt deshalb nur dann, wenn die Funkverbindung tatsächlich zustande kommt bzw. das CHO mit Standard-PMID unterstützt. Zusätzlich müssen bei den Belegungen die Kriterien für eine Aufenthaltsortaktualisierung erfüllt sein, d.h. ein LOCATE-Request empfangen oder die Sicherheitsmaßnahmen, Authentikation (und Ciphering), für den Link durchgeführt worden sein.
HDLC Error	Anzahl der nicht kritischen HDLC-Fehlermeldungen, die nicht an das Kommunikationssystem gemeldet wurden (Overflow, Underrun, CRC Error).
CMI Version	Hier wird die aktuelle Cordless-Version angezeigt.

Frequenz (Channel)	DECT	Europa 1880 – 1900 MHz	Latein-Amerika 1910 – 1930 MHz
10	9	1881,792 MHz	1911,16 MHz
9	8	1883,520 MHz	1912,896 MHz
8	7	1885,24 MHz	1914,624 MHz
7	6	1886,976 MHz	1916,352 MHz
6	5	1888,704 MHz	1918,080 MHz
5	4	1890,432 MHz	1919,80 MHz
4	3	1892,160 MHz	1921,536 MHz
3	2	1893,88 MHz	1923,264 MHz
2	1	1895,616 MHz	1924,992 MHz
1	0	1897,344 MHz	1926,720 MHz

27.2.4 Port/Baugruppen Zustand

Der Zustand aller Baugruppen kann angezeigt werden. Zusätzlich können die Baugruppen und ihre Ports freigegeben und gesperrt werden.

27.2.4.1 Port/Baugruppen Zustand > Baugruppen Zustand

Parameterbeschreibung der Registerkarten:

- **Baugruppen Zustand**

Parameter	Beschreibung
Slot	Physikalische Slotnummer.
Baugruppe	Bezeichnung der Baugruppe.
Nicht gesteckt	Angekreuzt, wenn Baugruppe nicht gesteckt ist.
Defekt	Angekreuzt, wenn Baugruppe defekt (nicht geladen) ist. Es ist auch möglich, dass eine defekte oder nicht konfigurierte Baugruppe nicht angezeigt wird.
Gesperrt	Angekreuzt ,wenn mindestens ein Port dieser Baugruppe gesperrt ist.
Frei	Angekreuzt ,wenn alle Ports dieser Baugruppe frei sind.
Belegt	Angekreuzt ,wenn mindestens ein Teilnehmer oder Leitung dieser Baugruppe abgehoben hat, gerufen wird oder im Gespräch ist.
Taktquelle	Angekreuzt, wenn die Baugruppe den Referenztakt liefert.
Schaltflächen	
Start	Aktualisierung der Anzeige wird gestartet. Der Zustand wird alle 3 Sekunden aktualisiert.
Stop	Aktualisierung der Anzeige wird gestoppt.

27.2.4.2 Port/Baugruppen Zustand > Out of Service

Parameterbeschreibung der Registerkarten:

- **Port out of Service**
- **Baugruppe out of Service**

Parameter	Beschreibung
Zugang	Einbauplatz und Port, an dem der Teilnehmer bzw. die Leitung angeschlossen ist.
Ruf-Nr.	Die dem Port zugeordnete Rufnummer.
Name	Der zum Teilnehmer bzw. zur Leitung gehörende Name.
Status	Je nachdem, ob am Port ein zugelassenes Endgerät oder eine zugelassene Leitung angeschlossen ist oder nicht, können die Ports **aktiv** oder **inaktiv** sein. Ports können auch im Zustand **in Betrieb** (Standardeinstellung) oder a**ußer Betrieb durch Tool** sein, d.h. dass sie über **Baugruppe sperren** gesperrt wurden. Der Zustand **in Betrieb** ist nicht identisch mit **aktiv**. Der Port-Status kann beispielsweise **aktiv**, **in Betrieb** oder auch **inaktiv**, **in Betrieb** sein.
Schaltflächen	
Auswahl sperren	Die markierten Ports werden gesperrt. Bei der Sperrung von $U_{P0/E}$ -Ports geht immer der zugehörige physikalische Port außer Betrieb. Dies hat zur Folge, dass bei Auswahl eines Master-Ports der zugehörige Slave-Port ebenfalls außer Betrieb geht.

Parameter	Beschreibung
Auswahl freigeben	Die markierten Ports werden freigegeben.
Baugruppe sperren	Die markierten Baugruppen und deren Ports werden gesperrt. Beim Sperren einzelner Mobiltelefone einer Cordless-Baugruppe wird immer die gesamte Baugruppe und somit auch alle Mobiltelefone gesperrt. Das Sperren einzelner Mobiltelefone wird durch Ändern der PIN der Mobiltelefone erreicht.
Baugruppe sperren	Die markierten Baugruppen und deren Ports werden freigegeben.

27.2.5 Traces

Unter **Traces** sind die Funktionen zum Tracen zusammengefasst. Der Administrator kann Traces starten und stoppen und die Trace-Einstellungen ändern.

27.2.5.1 Traces > Trace-Format-Konfiguration

Über die Trace-Format-Konfiguration wird definiert, welche Header-Daten in der Trace-Ausgabe enthalten sein sollen und wie die Trace-Daten formatiert werden sollen.

Parameterbeschreibung der Registerkarten:

- **Trace-Format-Konfiguration ändern**

Parameter	Beschreibung
In der Trace-Ausgabe enthaltene Header-Daten	
Globale Trace-Header Format-Einstellungen	Bei aktiviertem Flag können die Optionen für die nachfolgenden Header-Daten aktiviert oder deaktiviert werden. Standardwert: Aktiviert
Subsystem-ID	Bei aktiviertem Flag ist die Subsystem-ID in der Trace-Ausgabe enthalten. Standardwert: Aktiviert
Task-Name	Bei aktiviertem Flag ist der Task-Name in der Trace-Ausgabe enthalten. Standardwert: Aktiviert
Task-ID	Bei aktiviertem Flag ist die Task-ID in der Trace-Ausgabe enthalten. Standardwert: Aktiviert
Zeit	Bei aktiviertem Flag ist die Zeitangabe in der Trace-Ausgabe enthalten. Standardwert: Aktiviert
Modul-Name	Bei aktiviertem Flag ist der Modul-Name in der Trace-Ausgabe enthalten. Standardwert: Aktiviert
Zeilennummer	Bei aktiviertem Flag ist die Zeilennummer in der Trace-Ausgabe enthalten. Standardwert: Aktiviert

Parameter	Beschreibung
Aufbereitung der Trace-Daten (Formatierung)	
Volle Formatierung mit Parameterexpansion (Standard)	Standard-Ausgabemodus: Es werden alle Datentypen expandiert. Trace-Ausgabe: Normal (geeignet für den Normalbetrieb) Standardwert: Aktiviert
Eingeschränkt (Meldungstypen binär, speziell für Xtracer)	In diesem eingeschränkten Ausgabemodus werden die Datentypen im Binär-Format ausgegeben, das heißt so, wie sie zum Tracezeitpunkt vorliegen. Das Binär-Format ist für die Analyse mit dem X-Tracer-Tool bestimmt. Trace-Ausgabe: Schnell (geeignet für mittlere bis hohe Last) Standardwert: Deaktiviert
Eingeschränkt (nur Expansion elementarer Datentypen)	In diesem Ausgabemodus werden nur elementare Datentypen (zum Beispiel integer, short, long, string) expandiert. Trace-Ausgabe: Sehr schnell (geeignet für hohe Last) Standardwert: Deaktiviert
Performanceoptimierter Trace ohne Parameterexpansion	In diesem Ausgabemodus wird keine Datentyp-Expansion vorgenommen. Damit entsteht auch kein Aufwand für die Trace-Formatierung. Trace-Ausgabe: Extrem schnell (geeignet für sehr hohe Last) Standardwert: Deaktiviert

27.2.5.2 Traces > Trace-Ausgabe-Interfaces

Parameterbeschreibung der Registerkarten:

- **Ausgabe-Interfaces ändern**

Parameter	Beschreibung
Datei-Trace	
Datei-Trace aktivieren	Bei aktiviertem Flag werden Trace-Meldungen im Kommunikationssystem in eine Protokolldatei eingetragen. Standardwert: Aktiviert
Max. Trace-Quota (kByte)	Anzeige der maximalen Größe des Trace-Speichers in kByte
Strategie bei Erreichen der max. Quota	Auswahlmöglichkeit, was beim Erreichen der maximalen Trace-Quota passieren soll.
Strategie bei Erreichen der max. Quota: Wrap Around (lösche älteste Datei)	Beim Erreichen der maximalen Trace-Quota wird die jeweils älteste Trace-Protokolldatei überschrieben. Standardwert: Aktiviert
Strategie bei Erreichen der max. Quota: Datei-Trace wird temporär gestoppt	Beim Erreichen der maximalen Trace-Quota wird die Datei-Trace-Ausgabe gestoppt. Standardwert: Deaktiviert
Zeit, nach der jeweils eine neue Trace-Datei angelegt wird (s)	Anzeige der Zeit in Sekunden, nach deren Ablauf eine neue Trace-Protokolldatei angelegt wird.

Parameter	Beschreibung
Zeitraum für den Trace-Dateien verfügbar sind	Anzeige des Zeitraums, für den Trace-Protokolldateien verfügbar sind.
Trace über LAN (XTracer)	
Trace über LAN (XTracer) aktivieren	Trace-Meldungen werden über die LAN-Schnittstelle übertragen. Standardwert: Deaktiviert
Timer-Wert (s)	Anzeige der Zeit in Sekunden, nach deren Ablauf Trace-Daten übertragen werden.

27.2.5.3 Traces > Trace- Protokoll

Parameterbeschreibung der Registerkarten:

- **Laden über HTTP**
- **Trace-Protokoll löschen**

> ***INFO:*** Das Löschen von Trace-Protokolldaten kann nicht rückgängig gemacht werden.

Parameter	Beschreibung
Trace-Protokoll	
Gesamtes Protokoll	Alle vorhandenen Trace-Protokolldateien werden heruntergeladen.
Protokoll von heute	Trace-Protokolldateien des heutigen Tages (ab 00:00 Uhr) werden heruntergeladen.
Eigene Auswahl	Trace-Protokolldateien des ausgewählten Zeitraums werden heruntergeladen.

27.2.5.4 Traces > Digitale Prüfschleife

Die Konfiguration von digitalen Prüfschleifen ist ausschließlich mit Manager E möglich.

Digitale Prüfschleifen werden zur Leitungsüberprüfung von B-Kanälen der S_0-, S_{2M}- und T1-Schnittstellen eventuell vorhandener Baugruppen eingesetzt. Die Aktivierung digitaler Prüfschleifen sollte nur nach Aufforderung durch den Service-Provider erfolgen.

Parameterbeschreibung der Registerkarten:

- **Digital Loopback ändern**

27.2.5.5 Traces > Kunden-Trace-Protokoll

Mit dieser Funktion kann die Ereignis-Anzeige (Kunden-Trace) gestartet werden. Meldungstypen sind unter anderem System, SIP, STUN und LDAP.

Parameterbeschreibung der Registerkarten:

- **Anzeigen**
- **Laden über HTTP**
- **Trace-Protokoll löschen**

Parameter	Beschreibung
Autom. Aktualisierung	Bei aktiviertem Flag erfolgt eine automatische Aktualisierung der Anzeige des Kunden-Trace-Protokolls. Standardwert: Aktiviert
Sekunden bis zur nächsten Aktualisierung	Zeit in Sekunden nach deren Ablauf eine Aktualisierung des Kunden-Trace-Protokolls erfolgt.

27.2.5.6 Traces > M5T-Trace-Komponenten

Diese Funktion dient zur Überwachung des SIP-Stacks.

Änderungen der Einstellungen sollten nur nach Aufforderung durch den zuständigen Service-Support erfolgen.

Parameterbeschreibung der Registerkarten:

- **M5T-Trace-Komponenten bearbeiten**
- **Trace-Komponente starten/stoppen**

Parameter	Beschreibung
Package-Name	Name der M5T-Trace-Komponente
Trace-Level	Detailtiefe der Aufzeichnung der M5T-Trace-Komponente (Trace-Level 0 = geringste Detailtiefe bis Trace-Level 9 = größte Detailtiefe) Standardwert: 0
Trace an	Bei aktiviertem Flag erfolgt eine Aufzeichnung der Daten der M5T-Trace-Komponente. Standardwert: Deaktiviert
Crotch	Schrittweite der Aktivierung

27.2.5.7 Traces > Secure Trace

Diese Funktion dient zur Aufzeichnung von verschlüsselten VoIP-Nutz- und Signalisierungsdatenströmen.

Die Aufzeichnung verschlüsselter Verbindungsdaten erfordert zwingend die Zustimmung des Kunden und darf nur in Abstimmung mit dem zuständigen Service-Support vorgenommen werden. Informationen zur Vorgehensweise siehe Traces (Secure Trace)

HINWEIS: Das Aufzeichnen von Gesprächen und Verbindungsdaten ist ein Strafttatbestand, falls die betroffenen Teilnehmer nicht darüber informiert wurden.

Parameterbeschreibung der Registerkarten:

- **Secure Trace Passphrase ändern**
- **X.509-Datei für Secure Trace importieren**

Parameter	Beschreibung
Ändern der Secure Trace Aktivierungs- Passphrase	
Aktuelle Passphrase	Aktuelles Passwort (Passphrase) für das Starten und Stoppen des Secure Trace
Neue Passphrase	Neues Passwort (Passphrase) für das Starten und Stoppen des Secure Trace Wertebereich: 5 bis 12 Zeichen
Neue Passphrase wiederholen	Identisches neues Passwort (Passphrase) für das Starten und Stoppen des Secure Trace Wertebereich: 5 bis 12 Zeichen
Datei mit dem Zertifikat (PEM oder Binär-Format)	Auswahl der X.509-Datei, die das in das Kommunikationssystem zu importierende Zertifikat beinhaltet. Nach Auswahl der X.509-Datei kann der Fingerabdruck des zu importierenden Zertifikats angezeigt und anschließend das Zertifikat in das Kommunikationssystem importiert werden. ***INFO:*** Das Importieren des Zertifikat sollte nach der Prüfung des Fingerabdrucks erflogen.

27.2.5.8 Traces > Secure Trace > Secure Trace-Zertifikat

Diese Funktion dient zur Anzeige des importierten Secure Trace-Zertifikats.

Parameterbeschreibung der Registerkarten:

- **Secure Trace-Zertifikat anzeigen**

27.2.5.9 Traces > Secure Trace > Secure Trace-Einstellungen

Diese Funktion dient zur Statusabfrage und zum Starten/Stoppen des Secure Trace.

Parameterbeschreibung der Registerkarten:

- **Secure Trace Status**
- **Secure Trace starten/beenden**

Parameter	Beschreibung
Aktueller Secure Trace Status	
Secure Trace aktiviert	Status des Secure Trace
Automatischer Deaktivierungs-zeitpunkt	Zeit zu der der Secure Trace automatisch deaktiviert wird.
Secure Trace für folgende Protokolle	Anzeige der Protokolle, für die der Secure Trace erstellt wird.
Start Parameter	
Secure Trace Aktivierungs-Passphrase	Passwort (Passphrase) für das Starten und Stoppen des Secure Trace
Dauer des Secure Trace (Min.)	Zeitraum in Minuten in dem der Secure Trace aktiv sein soll. ***INFO:*** Die Eingabe eines Wertes ist unbedingt erforderlich.
Secure Trace für folgende Protokolle	
TC (TLS)	Bei aktiviertem Flag berücksichtigt der Secure Trace das TC (TLS)-Protokoll. Standardwert: Deaktiviert
H.323 Core/HSA (TLS)	Bei aktiviertem Flag berücksichtigt der Secure Trace das H.323 Core/HSA (TLS)-Protokoll. Standardwert: Deaktiviert
MMX (PEP)	Bei aktiviertem Flag berücksichtigt der Secure Trace das MMX (PEP)-Protokoll. Standardwert: Deaktiviert
SIP Core/SSA (TLS)	Bei aktiviertem Flag berücksichtigt der Secure Trace das SIP Core/SSA (TLS)-Protokoll. Standardwert: Deaktiviert
MSC (SRTP)	Bei aktiviertem Flag berücksichtigt der Secure Trace das MSC (SRTP)-Protokoll. Standardwert: Deaktiviert

27.2.5.10 Traces > Call Monitoring

Mit dieser Funktion kann die Überwachung von Leitungs- und Teilnehmerschnittstellen gestartet und gestoppt werden.

Parameterbeschreibung der Registerkarten:

- **Protokoll starten/stoppen**
- **Anzeigen**
- **Laden über HTTP**

Parameter	Beschreibung
Ausgewählter Port	Leitungs- oder Teilnehmerschnittstelle für die die Anrufüberwachung gestartet oder gestoppt werden soll.
Nr	Fortlaufende Nummer.
Time	Uhrzeit des Events (Ereignisses).
Callnumber/Access	Rufnummer und physikalische Schnittstelle.
State	Zustand der Schnittstelle. Möglich sind folgende Schnittstellenzustände: • Idle (Schnittstelle ist im Ruhezustand.) • Call Initiated (Schnittstelle ist bereit.) • Overlap Sending (externe Ziffernaussendung) • Outgoing Call Proc (Wahlende) • Call Request (Warten auf Alert) • Call Present (Schnittstelle wird gerufen.) • Active (Schnittstelle ist im Gesprächszustand.) • Hold (Schnittstelle ist im Zustand Halten.) • Disconnect Indication (Anforderung zum Trennen eines aktiven Gesprächs) • Direct (Schnittstelle ist im Modus Direktansprechen.) • Intrusion (Aufschalten wird aktiviert.) • Call Back A (Rückruf Teilnehmer A) • Call Back B (Rückruf Teilnehmer B) • Busy (Schnittstelle ist besetzt.) • Error (Fehler) • Disconnect PI (Warten auf Trennen von PI (Progress Indicator)) • Sensor (Signal wurde von Sensor ausgesendet.) • Conference Master (Konferenz-Master) • Paging (Personensuche) • Help Dial (Assoziierte Wahl wird verwendet.) • Remote (Schnittstelle durch Remote Service oder DISA belegt.) • ACD (Anrufverteilung) • Unknown State (unbekannter Zustand)

Parameter	Beschreibung
Event	Event (Ereignis) Möglich sind folgende Events: • Setup (Leitungsschnittstelle: Kommende oder gehende Belegung) • Setup Ackn (Leitungsschnittstelle: Belegungsquittung) • Info (Leitungsschnittstelle: Info (Rufnummernziffern)) • Call Proc (Leitungsschnittstelle: Unbewertetes Wahlende) • Progress (Leitungsschnittstelle: Zusatzinformation für Verbindungsaufbau) • Alert (Leitungsschnittstelle: Bewertetes Wahlende) • Connect (Leitungsschnittstelle: Anschaltung B-Kanal) • Connect Ackn (Leitungsschnittstelle: Quittung zu B-Kanal-Anschaltung) • Disconnect (Leitungsschnittstelle: Trenn-Anforderung) • Release (Leitungsschnittstelle: Trenn-Quittung) • Release Compl (Leitungsschnittstelle: Verbindung ausgelöst) • Monitor On (Leitungs-/Teilnehmerschnittstelle: Anrufüberwachung gestartet) • Monitor Off (Leitungs-/Teilnehmerschnittstelle: Anrufüberwachung gestoppt) • Off Hook (Teilnehmerschnittstelle: Hörer abgenommen) • On Hook (Teilnehmerschnittstelle: Hörer aufgelegt) • Digit (Teilnehmerschnittstelle: Ziffern werden gewählt)
Autom. Aktualisierung	Bei aktiviertem Flag erfolgt eine automatische Aktualisierung der Anzeige der Anrufüberwachung. Standardwert: Aktiviert
Sekunden bis zur nächsten Aktualisierung	Zeit in Sekunden nach deren Ablauf eine Aktualisierung der Anrufüberwachung erfolgt.

27.2.5.11 Traces > H.323-Stack-Trace

Diese Funktion dient zur Verfolgung von Problemen mit Komponenten, die das H.323-Protokoll nutzen.

Änderungen der Einstellungen sollten nur nach Aufforderung durch den zuständigen Service-Support erfolgen.

Parameterbeschreibung der Registerkarten:

- **H.323-Stack-Trace-Konfiguration ändern**
- **Alle H.323-Module ändern**
- **H.323-Stack-Trace-Protokoll über HTTP laden**
- **H.323 Stack-Trace-Protokoll löschen**

Parameter	Beschreibung
Allgemein	
Trace-Level	Detailtiefe der Aufzeichnung (Trace-Level 0 = geringste Detailtiefe bis Trace-Level 4 = größte Detailtiefe) Standardwert: 2
Konsolen-Trace	
Konsolen-Trace aktivieren	Bei aktiviertem Flag werden H.323-Stack-Trace-Meldungen auf der Konsole ausgegeben. Standardwert: Deaktiviert
Datei-Trace	
Datei-Trace aktivieren	Bei aktiviertem Flag werden H.323-Stack-Trace-Meldungen in eine Protokolldatei eingetragen. Standardwert: Deaktiviert
Max. Größe des Trace-Buffers (Byte)	Maximale Größe des Trace-Buffers in Byte (Menge der Daten, die im Zwischenspeicher gehalten wird.)
Max. Größe der Trace-Datei (Byte)	Maximale Größe der Trace-Protokolldatei in Byte
Trace-Timer (s)	Zeit in Sekunden, nach deren Ablauf Trace-Daten in die Protokolldatei geschrieben werden.
Modulname	Name des H.323-Stack-Trace-Moduls
Trace an	Bei aktiviertem Flag ist das H.323-Stack-Trace-Modul aktiv.

27.2.5.12 Traces > Lizenz-Komponente

Diese Funktion dient zur Überwachung des systeminternen Lizenzagenten CLA (Customer License Agent).

Änderungen der Einstellungen sollten nur nach Aufforderung durch den zuständigen Service-Support erfolgen.

Parameterbeschreibung der Registerkarten:

- **Ändern der CLA Trace Komponente**

Parameter	Beschreibung
Package-Name	Name der Lizenz-Trace-Komponente.
Trace-Level	Definition der Detailtiefe der Aufzeichnung der Lizenz-Trace-Komponente. Standardwert: Niedrig
Trace-Level: Niedrig	Niedrige Detailtiefe für die Trace-Aufzeichnung.
Trace-Level: Standard	Mittlere Detailtiefe für die Trace-Aufzeichnung.
Trace-Level: Alles	Hohe Detailtiefe für die Trace-Aufzeichnung.
Trace-Level: Aus	Lizenz-Trace-Komponente gestoppt.

27.2.5.13 Traces > Trace-Profile

Trace-Profile enthalten vordefinierte Trace-Komponenten zur Überwachung kompletter Funktionseinheiten des Kommunikationssystems.

Parameterbeschreibung der Registerkarten:

- **Alle Trace-Profile anzeigen**
- **Trace-Profil hinzufügen (leeres Profil)**
- **Trace-Profil hinzufügen (mit aktuellen Trace-Einstellungen)**
- **Alle Trace-Profile stoppen**
- **Trace-Profil starten/stoppen**

Parameter	Beschreibung
Profilname	Name des Trace-Profils
Profil gestartet	Anzeige, ob Trace-Profil gestartet wurde.
Profil schreibgeschützt	Anzeige, ob Trace-Profil schreibgeschützt ist (Alle standardmäßig vorhandenen Trace-Profile sind schreibgeschützt.).
Trace-Komponente	Name der Trace-Komponente
Enthalten	Bei aktiviertem Flag wird die Trace-Komponente in das neue, hinzuzufügende Trace-Profil übernommen. Standardwert: Aktiviert
Level	Detailtiefe der Aufzeichnung der Trace-Komponente (Trace-Level 0 = geringste Detailtiefe bis Trace-Level 9 = größte Detailtiefe)

27.2.5.14 Traces > Trace-Komponenten

Anhand von Trace-Komponenten werden die Prozess- und Zustandsinformationen einzelner Komponenten des Kommunikationssystems aufgezeichnet.

Parameterbeschreibung der Registerkarten:

- **Alle Trace-Komponenten anzeigen**
- **Gestartete Trace-Komponenten anzeigen**
- **Gestoppte Trace-Komponenten anzeigen**
- **Trace-Komponenten ändern**
- **Alle Trace-Komponenten stoppen**
- **Trace-Komponente starten/stoppen**

Parameter	Beschreibung
Subsystem-Name	Name der Trace-Komponente
Trace-Komponenten-Index	Fortlaufende Nummer
Trace-Level	Detailtiefe der Aufzeichnung (Trace-Level 0 = geringste Detailtiefe bis Trace-Level 9 = größte Detailtiefe)
Trace an	Bei aktiviertem Flag erfolgt eine Aufzeichnung der Daten der Trace-Komponente.

27.2.5.15 Traces > TCP- Dump

Ein TCP-Dump dient zur Überwachung und Auswertung des Datenverkehrs in einer IP-Vernetzung. Für die Diagnose der TCP-Dump-Dateien ist eine entsprechende Applikation erforderlich.

Parameterbeschreibung der Registerkarten:

- **Status TCP-Ausdruck**

Parameter	Beschreibung
TCP-Dump starten	Startet den TCP-Dump
Start-Parameter	
Schnittstellenname	Schnittstelle, für die eine Auswertung des Datenverkehrs erfolgt. Die verfügbaren Schnittstellen werden unter **Interface-Details** angezeigt. Der Eintrag **any** bewirkt eine Auswertung des Datenverkehrs für alle verfügbaren Schnittstellen. Standardwert: any
Paketgröße	Größe der Datenpakete in Byte, die aufgezeichnet werden sollen. Der Eintrag **0** bedeutet, jedes Paket wird komplett aufgezeichnet. Wertebereich: 0 - 2000000000, Standardwert: 0
Ende-Kriterien	
Anzahl der Pakete	Anzahl der Datenpakete, nach deren Erreichen der TCP-Dump beendet wird.
Zeit bis zur Beendigung (s)	Zeit in Sekunden, nach deren Ablauf der TCP-Dump beendet wird.
TCP-Dump beenden	Stoppen des TCP-Dump
TCP-Dump aufräumen	Löschen der im Kommunikationssystem gespeicherten TCP-Dump-Dateien
Autom. Aktualisierung	Bei aktiviertem Flag erfolgt eine automatische Aktualisierung der Statusanzeige. Standardwert: Aktiviert

27.2.5.16 Traces > rpcap Dämon

Ein RPCAP (Remote Packet Capture)-Dämon dient zur Überwachung und Auswertung des Datenverkehrs in einer IP-Vernetzung. Über den RPCAP-Dämon wird ein Fernzugriff externer Applikationen auf die TCP/IP-Pakete der

LAN-Schnittstellen des Kommunikationssystems ermöglicht. Ein RPCAP-Dämon wird häufig für Langzeit-Traces eingesetzt, da die Trace- Dateien auf einem PC und nicht im Kommunikationssystem abgelegt werden.

HINWEIS: Die in der Registerkarte genannten Sicherheitshinweise sind zu beachten.

Parameterbeschreibung der Registerkarten:

- **rpcap**

Parameter	Beschreibung
Adresse, an die gebunden werden soll	
IP-Adresse (numerisch oder literal)	IP-Adresse des HOST, auf dem die Aufzeichnungen erfolgen. Standardwert: 0.0.0.0
Port (bitte einen unbelegten Port auswählen)	Port des HOST, über den die Aufzeichnungen erfolgen.
Internes LAN tracen	Bei aktiviertem Flag erfolgt eine Aufzeichnung des Datenverkehrs zwischen zwei Baugruppen über die Schnittstelle eth9. Standardwert: Deaktiviert
Client-Identifikation für Zugriffskontrolle	
IP-Adresse (numerisch oder literal)	IP-Adresse des Remote-Clients, auf dem der Trace ausgegeben wird. Standardwert: 0.0.0.0

27.2.6 Events

Unter **Events** sind die Funktionen zum Anzeigen und Steuern der Ereignisse (Events) zusammengefasst. Dazu gehören z. B. die Event-Konfiguration und die E-Mail-Einstellungen.

27.2.6.1 Events > Event-Konfiguration

Parameterbeschreibung der Registerkarten:

- **Event-Konfiguration ändern**

Parameter	Beschreibung
Event-Datei-Einstellungen	
Max. Größe des Event-Buffers (Byte)	Anzeige der maximalen Größe des Event-Buffers in Byte
Max. Größe der Event-Datei (Byte)	Anzeige der maximalen Größe der Event-Protokolldatei in Byte

Parameter	Beschreibung
Event-Timer (s)	Anzeige der Zeit in Sekunden, nach deren Ablauf eine neue Event-Protokolldatei angelegt wird.
Event über LAN (XTracer)	
Event-Protokollierung über LAN (XTracer) aktivieren	Bei aktiviertem Flag werden Event-Protokollmeldungen über die LAN-Schnittstelle übertragen. Standardwert: Deaktiviert
Timer-Wert (s)	Anzeige der Zeit in Sekunden, nach deren Ablauf Event-Protokolldaten über die LAN-Schnittstelle übertragen werden.

27.2.6.2 Events > Event-Protokoll

Diese Funktion dient zum Herunterladen oder Löschen der Event-Protokolldatei.

Parameterbeschreibung der Registerkarten:

- **Laden über HTTP**
- **Event-Protokoll löschen**

27.2.6.3 Events > E-Mail

Parameterbeschreibung der Registerkarten:

- **E-Mail-Einstellungen bearbeiten**

Parameter	Beschreibung
E-Mail-Einstellungen	
Betreff	Text, der im Betreff-Feld der E-Mails angezeigt wird.
Empfänger-E-Mail-Adressen	
Empfänger 1	E-Mail-Adresse, an die eine E-Mail bei Eintreten eines Events verschickt wird.
Empfänger 2	E-Mail-Adresse, an die eine E-Mail bei Eintreten eines Events verschickt wird.
Empfänger 3	E-Mail-Adresse, an die eine E-Mail bei Eintreten eines Events verschickt wird.
Empfänger 4	E-Mail-Adresse, an die eine E-Mail bei Eintreten eines Events verschickt wird.
Empfänger 5	E-Mail-Adresse, an die eine E-Mail bei Eintreten eines Events verschickt wird.

27.2.6.4 Events > Reaktionstabelle

Anhand der Reaktionstabelle kann für jeden möglichen Event getrennt definiert werden, wie bei dessen Eintreten reagiert werden soll.

Parameterbeschreibung der Registerkarten:

- **Alle Events ändern**

- **Alle Events auf Werkseinstellung zurücksetzten**
- **Event bearbeiten**
- **Zugeordnetes Trace-Profil starten/stoppen**

Parameter	Beschreibung
Event-Name	Name des Events
SNMP-Trap senden	Bei aktiviertem Flag wird bei Eintreten des Events ein SNMP-Trap gesendet.
E-Mail versenden	Bei aktiviertem Flag wird bei Eintreten des Events eine E-Mail an die unter **E-Mail-Einstellungen bearbeiten** eingetragenen E-Mail-Empfänger verschickt.
Zugeordnetes Trace-Profil	Trace-Profil, das bei Eintreten des Events gestartet oder gestoppt wird.
Trace-Profil starten	Bei aktiviertem Flag wird bei Eintreten des Events das ausgewählte Trace-Profil gestartet.
Trace-Profil stoppen	Bei aktiviertem Flag wird bei Eintreten des Events das ausgewählte Trace-Profil gestoppt.
Gateway neu starten	Zeigt an, ob bei Eintreten des Events das Kommunikationssystem neu gestartet wird.
Gateway neu starten: Ja	Bei Eintreten des Events erfolgt ein Neustart des Kommunikationssystems.
Gateway neu starten: Nein	Bei Eintreten des Events erfolgt kein Neustart des Kommunikationssystems.
OpenScape benachrichtigen	Zeigt an, ob bei Eintreten des Events eine Meldung an das Kommunikationssystem erfolgt.
OpenScape benachrichtigen: Ja	Bei Eintreten des Events erfolgt eine Meldung an das Kommunikationssystem.
OpenScape benachrichtigen: Nein	Bei Eintreten des Events erfolgt keine Meldung an das Kommunikationssystem.

27.2.6.5 Events > Diagnose Logs

Hier werden die Diagnose Logs ((Protokolldateien) angezeigt, die bei kritischen Systemzuständen automatisch erzeugt wurden.

Parameterbeschreibung der Registerkarten:

- **Diagnose Logs holen**
- **Diagnose Logs löschen**

Parameter	Beschreibung
Dateiname	Name des im Kommunikationssystem gespeicherten Diagnose Logs ((Protokolldatei)
Größe (in Byte)	Größe der Diagnose Logs in Byte
Geändert	Änderungsdatum des Diagnose Logs
Attribute	Attribute des Diagnose Logs: • r = Leseberechtigung (Read) • w = Schreibberechtigung (Write)

27.2.6.6 Events > Alarm-Signalisierung

Hier werden die Teilnehmer (Systemtelefone mit Display, UP0 & HFA) ausgewählt, die benachrichtigt werden, wenn die Temperatur des Systems 55 Grad Celsius übersteigt. Werden 60 Grad Celsius überschritten, werden die für die Überhitzung verantwortlichen Baugruppen (z. B. OCAB, SLAD8/16) kontrolliert heruntergefahren oder abgeschaltet.

Parameterbeschreibung der Registerkarten:

- **Alarm-Signalisierung ändern**

Parameter	Beschreibung
Temperatur Alarm-Siganlisierungsports	
Teilnehmer 1	1. Ziel (Teilnehmer mit Systemtelefon).
Teilnehmer 2	2. Ziel (Teilnehmer mit Systemtelefon).
Teilnehmer 3	3. Ziel (Teilnehmer mit Systemtelefon).

27.2.7 Restart / Reload

Hier kann ein Restart (Neustart) oder ein Reload von OpenScape Business ausgelöst werden oder OpenScape Business X kontrolliert herunterfahren werden (Shutdown). Darüber hinaus kann ein Restart (Neustart) der UC Applikation (UC Smart oder UC Suite) oder der UC Booster Card (Application Board OCAB) ausgelöst werden. Um das kontrollierte Herunterfahren von OpenScape Business X über ein Systemtelefon zu ermöglichen, kann eine PIN definiert werden. Im Fall einer Vernetzung ist die Synchronisierung der vernetzten Kommunikationssysteme möglich.

27.2.7.1 Restart / Reload > Restart / Reload

Parameter	Beschreibung
System	
System neu starten	Kontrollierter Restart (Neustart) von OpenScape Business: • OpenScape Business S und OpenScape Business X: Es erfolgt ein kontrollierter Restart (Neustart) des Kommunikationssystems. Ist OpenScape Business X3/X5/X8 mit einer UC Booster Card (Application Board OCAB) bestückt, erfolgt auch ein kontrollierter Restart (Neustart) der UC Applikation (UC Smart oder UC Suite). • OpenScape Business UC Booster Server (Application Server): Es erfolgt ein kontrollierter Restart (Neustart) des OpenScape Business-Anteils und der UC Applikation (UC Suite).
System-Reload ausführen	Reload von OpenScape Business: • OpenScape Business S und OpenScape Business X: Es erfolgt ein Reload des Kommunikationssystems. Nach dem anschließenden Hochlauf befindet sich das Kommunikationssystem im Grundzustand. Alle länder- und kundenspezifischen Einstellungen wurden gelöscht (System-Länderkennzeichen = Deutschland). Das Kommunikationssystem hat die Standard-IP-Adresse 192.168.1.2 und den internen IP-Adressbereich 192.168.3.xxx. Die Lizenzierung bleibt erhalten. • OpenScape Business UC Booster Server: Es erfolgt ein Reload des OpenScape Business-Anteils. Nach dem anschließenden Hochlauf befindet sich der OpenScape Business-Anteil im Grundzustand. Alle kundenspezifischen Einstellungen des OpenScape Business-Anteils (zum Beispiel das Benutzerverzeichnis) wurden gelöscht. Die Lizenzierung bleibt erhalten. Das Betriebssystem wird nicht zurückgesetzt.
System herunterfahren	Kontrolliertes Herunterfahren von OpenScape Business X: • OpenScape Business X3/X5: Das anschließende Hochfahren des Kommunikationssystems ist ausschließlich durch Ziehen und anschließendes Stecken des Netzsteckers möglich. • OpenScape Business X8: Das anschließende Hochfahren des Kommunikationssystems ist ausschließlich durch Ausschalten und anschließendes Wiedereinschalten aller Stromversorgungen LUNA2 möglich.
Shutdown aktivieren/deaktivieren	Definition einer PIN für die Aktivierung des Shutdowns (das kontrollierte Herunterfahren des Kommunikationssystems) über ein Systemtelefon
Application Board neu starten	Kontrollierter Restart (Neustart) des Application Boards OCAB inklusive der UC Applikation (UC Smart oder UC Suite): Bei einem Restart des Application Boards OCAB werden die Verbindungen zu allen aktiven Anwendungen, wie zum Beispiel myPortal for Desktop, myPortal Smart und myAttendant, getrennt. Nach dem Hochlauf werden alle Verbindungen automatisch wiederhergestellt.

Parameter	Beschreibung
Applikationen	
Sync-Netzwerk	Synchronisierung vernetzter Kommunikationssysteme: Nach der Änderung von Rufnummern, Durchwahlnummern oder Namen werden durch eine Synchronisierung die Daten in allen vernetzten Kommunikationssystemen aktualisiert.
UC Application neu starten	Kontrollierter Restart (Neustart) der UC Applikation (UC Smart oder UC Suite): Bei einem Restart der UC Applikation werden die Verbindungen zu allen aktiven Anwendungen, wie zum Beispiel myPortal for Desktop, myPortal Smart und myAttendant, getrennt. Nach dem Hochlauf werden alle Verbindungen automatisch wiederhergestellt.

27.2.8 SNMP

Unter **SNMP** sind die Funktionen zum Einrichten von Communities und Traps zusammengefasst. Durch Communities werden die Zugriffsberechtigungen auf die SNMP-Daten geregelt. Bei Problemen im System werden Traps erzeugt, um den Administrator über Fehler und Ausfälle zu informieren.

27.2.8.1 SNMP > Communities

Parameterbeschreibung der Registerkarten:

- **Communities anzeigen**

Parameter	Beschreibung
IP-Adresse	IP-Adresse des SNMP-Kommunikationspartners. Bei der Adresse 127.0.0.1 ist die Kommunikation mit externen IP-Adressen gesperrt.
Community	Identifikation/Zugangspasswort, das für den SNMP-Nutzer verwendet wird. ***INFO:*** Zur Erhöhung der Sicherheit wird empfohlen, nicht den Standardwert **public** zu verwenden.
Typ	Auswahl des Typs.
Typ: Lesende Community	Kommunikationspartner mit lesendem SNMP-Zugang.
Typ: Schreibende Community	Kommunikationspartner mit lesendem und schreibendem SNMP-Zugang.
Typ: Trap-Community	Kommunikationspartner, an den Fehlermeldungen (Traps) gesendet werden.

27.2.8.2 SNMP > Communities > Lesende Communities

Parameterbeschreibung der Registerkarten:

- **Lesende Communities anzeigen**
- **Lesende Community hinzufügen**

Parameter	Beschreibung
IP-Adresse	IP-Adresse des SNMP-Kommunikationspartners. Bei der Adresse 127.0.0.1 ist die Kommunikation mit externen IP-Adressen gesperrt.
Community	Identifikation/Zugangspasswort, das für den SNMP-Nutzer verwendet wird. ***INFO:*** Zur Erhöhung der Sicherheit wird empfohlen, nicht den Standardwert **public** zu verwenden.

27.2.8.3 SNMP > Communities > Schreibende Communities

Parameterbeschreibung der Registerkarten:

- **Schreibende Communities anzeigen**
- **Schreibende Community hinzufügen**

Parameter	Beschreibung
IP-Adresse	IP-Adresse des SNMP-Kommunikationspartners. Bei der Adresse 127.0.0.1 ist die Kommunikation mit externen IP-Adressen gesperrt.
Community	Identifikation/Zugangspasswort, das für den SNMP-Nutzer verwendet wird. ***INFO:*** Zur Erhöhung der Sicherheit wird empfohlen, nicht den Standardwert **public** zu verwenden.

27.2.8.4 SNMP > Communities > Trap Communities

Parameterbeschreibung der Registerkarten:

- **Trap-Communities anzeigen**
- **Trap-Community hinzufügen**

Parameter	Beschreibung
IP-Adresse	IP-Adresse des SNMP-Kommunikationspartners. Bei der Adresse 127.0.0.1 ist die Kommunikation mit externen IP-Adressen gesperrt.
Community	Identifikation/Zugangspasswort, das für den SNMP-Nutzer verwendet wird. ***INFO:*** Zur Erhöhung der Sicherheit wird empfohlen, nicht den Standardwert **public** zu verwenden.

27.2.8.5 SNMP > Traps

Parameterbeschreibung der Registerkarten:

- **Alle Traps anzeigen**
- **Alle kritischen Traps anzeigen**

Parameter	Beschreibung
VarBind1 (Severity)	Klassifizierung des Traps: • Critical: Fehlermeldung. Der Fehler hat problematische Auswirkungen. • Major: Fehlermeldung. Der Fehler kann problematische Auswirkungen haben. • Minor: Fehlermeldung. Der Fehler hat keine problematischen Auswirkungen. • Warning: Meldung über einen möglicherweise problematischen Vorgang oder Zustand. • Cleared: Die Fehlermeldung wurde aufgehoben (zum Beispiel Port ist wieder in Betrieb) • Information: Reine Statusmeldung, keine Fehlermeldung
VarBind2 (Name)	Name des Traps
Generischer Name	Allgemeine Bezeichnung, wie zum Beispiel Enterprise Specific
Spezifischer Name	Typ des Traps: • 1 = Software • 2 = Hardware
Enterprise	(nicht genutzt)
Zeit	Zeitpunkt des Fehlers
Index	Fortlaufende Nummer

27.2.9 Admin-Protokoll

Mit **Admin.-Protokoll** kann der Administrator die Konfiguration (z. B. die Sprache) für das Administrationsprotokoll ändern.

27.2.9.1 Admin-Protokoll > Konfiguration

Parameterbeschreibung der Registerkarte:

- **Konfiguration ändern**

Parameter	Beschreibung
Admin-Protokoll Sprache	Einstellung der gewünschten Sprache für das Admin-Protokoll. Das Admin-Protokoll bietet eine Übersicht der am Kommunikationssystem durchgeführten Änderungen. Mögliche Sprachen: Deutsch, Englisch, Französisch, Spanisch, Italienisch, Portugiesisch, Niederländisch

27.2.9.2 Admin-Protokoll > Admin.-Protokoll-Daten

Parameterbeschreibung der Registerkarte:

- **Laden über HTTP**

Parameter	Beschreibung
Laden über HTTP	Speichert des Admin-Protokoll des Kommunikationssystems. Das Admin-Protokoll gibt Auskunft, wann Änderungen am Kommunikationssystem durchgeführt worden sind und von wem diese gemacht wurden. Protokolliert werden die Logins auf dem Kommunikationssystem.

27.2.10 Aktionen

Unter **Aktionen** sind die Funktionen zusammengefasst, die den Administrator bei häufig wiederkehrenden Administrationsaufgaben z. B. dem Löschen von Protokolldaten unterstützen.

27.2.10.1 Aktionen > Manuelle Aktionen > Diagnose-Protokolle

Parameterbeschreibung der Registerkarten:

- **Daten laden über HTTP**

Parameter	Beschreibung
Trace-Protokoll	Bei aktiviertem Flag werden Systemtrace-Protokolldateien heruntergeladen. Folgende Auswahlmöglichkeiten bestehen: • Gesamtes Protokoll: Die gesamten vorhandenen Systemtrace-Protokolldateien werden heruntergeladen. • Protokoll von heute: Die Systemtrace-Protokolldateien des heutigen Tages (ab 00:00 Uhr) werden heruntergeladen. • Eigene Auswahl: Von: XXX Bis: YYY: Die Systemtrace-Protokolldateien des ausgewählten Zeitraums werden heruntergeladen. Standardwert: Aktiviert, Gesamtes Protokoll
Event-Protokoll	Bei aktiviertem Flag werden Protokolldateien mit Angaben über Aktionen/Events des Kommunikationssystems (Reset, Ein-/Ausschalten usw.) heruntergeladen. Standardwert: Aktiviert
Admin-Protokoll	Bei aktiviertem Flag werden Protokolldateien mit Angaben über Administrationsvorgänge (Login-Versuche usw.) heruntergeladen. Standardwert: Aktiviert
Lizenzprotokolle	Bei aktiviertem Flag werden Protokolldateien mit Meldungen über lizenzierungspflichtige Komponenten des Kommunikationssystems heruntergeladen. Standardwert: Aktiviert
Kunden-Trace	Bei aktiviertem Flag werden Protokolldateien mit Meldungen für den Kunden-Trace (Remote-Login, ITSP-Login usw.) heruntergeladen. Die Meldungen für den Kunden-Trace werden dabei in ausführlicherer Form dargestellt, als zum Beispiel im Trace-Protokoll. Standardwert: Aktiviert

Parameter	Beschreibung
Framework-Protokoll	Bei aktiviertem Flag werden Protokolldateien mit Meldungen des WBM heruntergeladen. Standardwert: Aktiviert
Diagnoseprotokoll	Bei aktiviertem Flag werden Diagnose Logs des Kommunikationssystems heruntergeladen. Standardwert: Aktiviert
UC Suite-Protokolle	Bei aktiviertem Flag werden Protokolldateien mit Meldungen der UC Suite (UC Suite-, CSP- und MEB-Protokolle) heruntergeladen. Folgende Auswahlmöglichkeiten bestehen: • Gesamtes Protokoll: Alle vorhandenen UC Suite-, CSP- und MEB-Protokolldateien werden heruntergeladen. • Protokoll von heute: Die UC Suite-, CSP- und MEB-Protokolldateien des heutigen Tages (ab 00:00 Uhr) werden heruntergeladen. • Eigene Auswahl: Von: XXX Bis: YYY: Die UC Suite-, CSP- und MEB-Protokolldateien des ausgewählten Zeitraums werden heruntergeladen. Alle Protokolldateien werden in einer komprimierten Datei zusammengefasst. Für die OpenScape Business-Protokolle gelten folgende Dateibezeichnungen: UC Suite-Protokolldateien = vs_jjjj_mm_tt.log, CSP-Protokolldateien = csptrace_jjjj_mm_tt.log, MEB-Protokolldateien = mebtrace_jjjj_mm_tt.log Standardwert: Deaktiviert
Applikationsprotokolle	Bei aktiviertem Flag werden Protokolldateien mit Meldungen des Applikationsanteils des Kommunikationssystems (zum Beispiel CSP-Protokolle) heruntergeladen. • Gesamtes Protokoll: Alle vorhandenen Protokolldateien werden heruntergeladen. • Protokoll von heute: Die Protokolldateien des heutigen Tages (ab 00:00 Uhr) werden heruntergeladen. • Eigene Auswahl: Von: XXX Bis: YYY: Die Protokolldateien des ausgewählten Zeitraums werden heruntergeladen. Alle Protokolldateien werden in einer komprimierten Datei zusammengefasst. Standardwert: Deaktiviert
System-Diagnose-Protokolle	Bei aktiviertem Flag werden Diagnose-Protokolle des Kommunikationssystems heruntergeladen. Standardwert: Aktiviert
PPP-Protokoll	Bei aktiviertem Flag werden Protokolldateien mit Meldungen zum Point-to-Point-Protokoll heruntergeladen. Standardwert: Aktiviert
CoreLog-Protokoll	Bei aktiviertem Flag werden Protokolldateien mit Informationen über den letzten Zustand des Betriebssystems heruntergeladen. CoreLogs werden zum Beispiel bei Restarts erstellt. Standardwert: Deaktiviert

27.2.10.2 Aktionen > Automatische Aktionen > Garbage Collection

Parameterbeschreibung der Registerkarten:

- **Aktion ändern**

- **Aktion starten/stoppen**

Parameter	Beschreibung
Aktion aktiviert	Bei aktiviertem Flag wird regelmäßig eine automatische Speicherbereinigung auf dem Kommunikationssystem durchgeführt. Nach Abschluss jeder Speicherbereinigung führt das Kommunikationssystem einen Restart (Neustart) durch. Standardwert: Deaktiviert
Startzeit nach Mitternacht	Zeitpunkt nach Mitternacht, an dem die Aktion Garbage Collection durchgeführt wird. Beispiel: Im Feld **Std.** wurde 3 und im Feld **Min.** 30 eingegeben. Das bedeutet, die Aktion Garbage Collection wird morgens um 3:30 Uhr gestartet. Standardwert: 3 Std. 00 Min.
Aktion an folgenden Wochentagen ausführen	Die Aktion Garbage Collection wird an den ausgewählten Wochentagen durchgeführt. Standardwert: Aktiviert

27.2.10.3 Aktionen > Automatische Aktionen > DLS Notification

Parameterbeschreibung der Registerkarten:

- **Aktion ändern**
- **Aktion starten/stoppen**

Parameter	Beschreibung
Aktion aktiviert	Bei aktiviertem Flag wird beim Hochlauf des Kommunikationssystems die automatische Anmeldung an einem externen DLS-Server initiiert. Standardwert: Deaktiviert
IP-Adresse	IP-Adresse des externen DLS-Servers Standardwert: 0.0.0.0
Port	Port des externen DLS-Servers Standardwert: 10444
Benutzername	Benutzername für die Anmeldung am externen DLS-Server
Passwort	Passwort für die Anmeldung am externen DLS-Server

27.2.11 Plattform-Diagnose

Möglichkeit der Plattform-Diagnose (nur für Entwicklung).

27.2.12 Applikat.-Diagnose

Möglichkeit der Applikations-Diagnose (nur für Entwicklung).

27.2.12.1 Applikat.-Diagnose > Entwickler-Einstellungen > Trace-Konsolen-Ausgabe

Möglichkeit der Applikations-Diagnose (nur für Entwicklung).

27.2.12.2 Applikat.-Diagnose > Entwickler-Einstellungen > Übernahme des Write Tokens

Möglichkeit der Applikations-Diagnose (nur für Entwicklung).

27.2.12.3 Applikat.-Diagnose > Mainboard

Änderungen der Einstellungen sollten nur nach Aufforderung durch den zuständigen Service-Support erfolgen.

27.2.13 IP-Diagnose

Möglichkeit der IP-Diagnose (nur für Entwicklung).

27.2.13.1 IP-Diagnose > Mainboard > ARP-Protokoll

Diese Funktion dient zur Anzeige der Daten des Address Resolution Protocol ARP. Die Mapping-Tabelle zeigt die Zuordnung der Netzwerkadressen zu den MAC-Adressen.

Parameterbeschreibung der Registerkarten:

- **ARP-Protokoll anzeigen**

Parameter	Beschreibung
IP-Adresse	Zeigt die Netzwerkadressen, die aktuell am Mainboard des Kommunikationssystems angeschlossen sind.
MAC-Adresse	Zeigt die zugehörige physikalische Adresse des angeschlossenen Netzwerkadressen
Typ	Zeigt die Zuordnung der Adressen. Möglich ist eine feste (statisch) oder dynamische Zuordnung.
Schnittstelle	Interne Bezeichnung der vorhandenen LAN-Schnittstellen (zum Beispiel eth0, eth1, eth2, eth3)

27.2.13.2 IP-Diagnose > Mainboard > ICMP-Anforderung > Ping

Mittels dieser Funktion kann die Netzwerkverbindung zwischen dem Kommunikationssystem und einer frei wählbaren Ziel-Adresse mit Hilfe eines Ping-Befehls (Echoanforderung) überprüft werden.

Parameterbeschreibung der Registerkarten:

- **Execute Ping**

Parameter	Beschreibung
ICMP-Parameter	
Ziel-Adresse	IP-Adresse des Ziels, dessen Netzwerkverbindung zum Kommunikationssystem mit Hilfe von Echoanforderungspaketen überprüft wird. Standardwert: 127.0.0.1
Anzahl zu sendender Echoanforderungen	Anzahl der zu sendenden Echoanforderungspakete für die Überprüfung der Netzwerkverbindung Standardwert: 3

27.2.13.3 IP-Diagnose > Mainboard > ICMP-Anforderung > Traceroute

Mittels dieser Funktion wird anhand von ICMP-Echoanforderungen ermittelt, über welche Router Datenpakete bis zur abgefragten Ziel-Adresse vermittelt werden.

Parameterbeschreibung der Registerkarten:

- **Traceroute**

Parameter	Beschreibung
ICMP-Parameter	
Ziel-Adresse	IP-Adresse des Ziels, dessen Traceroute zum Kommunikationssystem mit Hilfe von ICMP-Echoanforderungen überprüft wird. Standardwert: 127.0.0.1
TOS-Byte	Anzeige, ob TOS (Type Of Service)-Bytes gesendet werden. TOS-Bytes geben Aufschluss über die Qualität eines Dienstes. Wertebereich: 0 bis 255, Standardwert: 0

27.2.14 Online-Benutzer

Web-Tool zur Fernsteuerung von OpenStage-Telefonen.

27.2.14.1 Online Benutzer

Mit dem Online-Benutzer öffnet sich der Java Husim Phone Tester (jHPT). Dies ist ein Web-Tool zur Fernsteuerung von OpenStage-Telefonen über das Internet. Über eine Web-Oberfläche wird ein vorhandenes Systemtelefon so kontrolliert, dass reale Tastendrücke und Anzeigen des Kommunikationssystems übermittelt werden. Für das jHPT gibt es eine separate Dokumentation, die über die Hilfe-Funktion des Tools heruntergeladen werden kann (hier keine weitere Beschreibung der jHPT Seiten).

27.3 Telefonie

Unter **Telefonie** sind Funktionen für die Konfiguration der Telefonie zusammengefasst, um z. B. Teilnehmer oder das Call Management (CM) einzurichen.

27.3.1 Grundeinstellungen

Unter **Grundeinstellungen** sind Funktionen zusammengefasst, wie z. B. Systemflags, Einstellungen für Verzeichnisse und Kurzwahlziele, DynDNS, Quality of Service, Datum und Uhrzeit und Gebühren.

27.3.1.1 Grundeinstellungen > System > System Flags

Parameterbeschreibung der Registerkarten:

- **System Flags ändern**

Parameter	Beschreibung
Durchschalten bei AUL extern ein	Bei aktiviertem Flag wird ein Anruf bei einer externen Anrufumleitung sofort durchgeschaltet. Das Durchschalten erfolgt unabhängig davon, ob es sich um einen internen oder externen (HKZ/ISDN) Anruf handelt. Erfolgt die Anrufumleitung über eine ISDN-Amtsleitung und befindet sich das externe Anrufumleitungsziel in einem anderen Netz (zum Beispiel GSM-Netz), wird der Verbindungsaufbau vom ISDN-Amt mit dem Progress-Indikator Leaving ISDN gemeldet. Ab diesem Zeitpunkt entstehen Verbindungskosten für den Anrufer. Standardwert: Deaktiviert
Anrufumleitung nach HKZ erlaubt	Bei aktiviertem Flag folgen Anrufe über analoge Amtleitungen (HKZ) der externen Anrufumleitung. Standardwert: Aktiviert
Rufweiterschaltung nach AUL zum externen Ziel	Bei aktiviertem Flag gilt: Ist das externe Anrufumleitungsziel nicht erreichbar, erfolgt eine Rufweiterschaltung zum nächsten in der Rufzielliste eingetragenen Ziel. Standardwert: Deaktiviert
Konferenzton	Bei aktiviertem Flag werden die Teilnehmer einer Konferenz im Abstand von 20 Sekunden durch einen Sonderton darauf aufmerksam gemacht, dass sie sich in einer Konferenz befinden. Standardwert: Deaktiviert
Aufmerksamkeitssignalisierung bei AUN-Gruppen	Bei aktiviertem Flag wird ein Anruf für ein Mitglied einer Anrufübernahmegruppe bei den anderen Gruppenmitglieder optisch (Display) signalisiert. Wird der Anruf nicht innerhalb von vier Rufzyklen (4 x 5 Sekunden) angenommen, erhalten die anderen Gruppenmitglieder zusätzlich einen Aufmerksamkeitston. Standardwert: Aktiviert
Sprachlautstärke für optiPoint/ OpenStage erhöhen	Bei aktiviertem Flag wird für die optiPoint- und OpenStage-Telefone auf einen alternativen Dämpfungsplan umgeschaltet und damit eine höhere Sprachlautstärke erzielt. Standardwert: Deaktiviert

Parameter	Beschreibung
Endgerätetausch erlaubt	Bei aktiviertem Flag können Systemtelefone ohne Veränderung der logischen Konfiguration (Rufnummer, Name, Tastenprogrammierung usw.) physikalisch umgesteckt werden (Relocate/Rufnummerntausch). Standardwert: Deaktiviert
Mehr als 1 externer Konferenzteilnehmer	Bei aktiviertem Flag können mehrere externe Teilnehmer an einer Konferenz teilnehmen. Standardwert: Aktiviert
automatisches Leitungsvormerken	Bei aktiviertem Flag kann ein Teilnehmer eine Leitung vormerken, wenn ihm keine freie Amtsleitung zur Verfügung steht. Sobald diese Leitung frei wird, erhält er einen Wiederanruf und kann anschließend die externe Verbindung aufbauen. Standardwert: Deaktiviert
Wahlwiederholung mit PKZ	Bei aktiviertem Flag wird bei der Wahlwiederholung neben der Rufnummer auch eine vorher eingegebene PKZ wiederholt. Standardwert: Deaktiviert
Nur eingerichtete Nummer für MSN benutzen	Bei aktiviertem Flag können an einem S0-Bus die MSN (Multiple Subscriber Number) nur für bereits vorhandene interne Rufnummern eingerichtet werden (um eventuellen Gebührenmissbrauch zu verhindern). Standardwert: Deaktiviert
Wegeoptimierung	Bei aktiviertem Flag wird bei vernetzten Kommunikationssystemen eine Wegeoptimierung durchgeführt. Das Flag muss bei allen zu einer Vernetzung gehörenden Kommunikationssystemen aktiviert werden. Beispiel für zwei vernetzte Systeme (System 1 und System 2): Bei einem Anruf von Teilnehmer A (System 1) nach Teilnehmer B (System 2) und anschließender Anrufumleitung zu Teilnehmer C (System 1) werden zwei Leitungen belegt. Durch Wegeoptimierung wird die Verbindung von A nach C automatisch über eine einzige Leitung geschaltet. Standardwert: Aktiviert
DTMF automatisch	Bei aktiviertem Flag wird nach jedem erfolgreichen gehenden Verbindungsaufbau automatisch in den DTMF-Modus (MFV-Modus) umgeschaltet. Damit wird zum Beispiel die Fernabfrage von Anrufbeantwortern ermöglicht. Standardwert: Aktiviert
Paging mit Zweierverbindung	Bei aktiviertem Flag ermöglicht Direktansprechen (Paging) einen internen Verbindungsaufbau, ohne dass der gerufene Teilnehmer den Hörer abhebt. Durch Abheben des Hörers erfolgt der Übergang zu einem normalen Zweiergespräch. Standardwert: Aktiviert
Ton vom Amt	Bei aktiviertem Flag wird eine Verbindung auch dann zum Amt oder zu einem vernetzten Kommunikationssystem durchgeschaltet, wenn von der Gegenseite kein Ton gesendet wird. Standardwert: Deaktiviert
R-Gesprächsschutz	Bei aktiviertem Flag werden R-Gespräche automatisch ausgelöst. Standardwert: Deaktiviert

Parameter	Beschreibung
Euroimpedanz (nur für bestimmte Länder)	Bei aktiviertem Flag gelten folgende Impedanzwerte in Europa: a/b-Schnittstellen für den analogen Teilnehmeranschluss: Eingangsimpedanz = 270 Ohm + 750 Ohm || 150 nF, Nachbildimpedanz = 270 Ohm + 750 Ohm || 150 nF, Relativer Pegel A/D = 0 dBr, Relativer Pegel D/A = –7 dBr a/b-Schnittstellen für den analogen Amtsanschluss: Eingangsimpedanz = 270 Ohm + 750 Ohm || 150 nF, Nachbildimpedanz = 270 Ohm + 750 Ohm || 150 nF, Relativer Pegel A/D = –6 dBr, Relativer Pegel D/A = –1 dBr Standardwert: Deaktiviert
Verschiedene Phonemailansagen Tag/Nacht	Bei aktiviertem Flag können (bei einem Kommunikationssystem mit Voicemail) verschiedene Voicemail-Ansagen für einen Teilnehmer aktiviert werden, indem verschiedene Rufnummern für diesen Teilnehmer an die Voicemail übermittelt werden. Voraussetzung dafür ist, dass für diesen Teilnehmer unterschiedlich Rufweiterschaltungen für Tag- und Nachtbetrieb konfiguriert werden. Standardwert: Deaktiviert
Internationale/nationale Kennzahl anzeigen	Bei aktiviertem Flag wird das Anzeigeformat von KWZ-Nummern bei kommenden Anrufen definiert, für die im KWZ-Speicher kein Name hinterlegt ist. Im Display des Telefons wird bei kommenden Anrufen die komplette Rufnummer angezeigt (Anlagenrufnummer + Durchwahl, inklusive Ortsnetzkennzahl und Ländervorwahl, falls vorhanden). Beispiel: Die KWZ-Nummer 06671234 wurde ohne Namen eingerichtet. Ortsnetzkennzahl = 02302, Anlagenrufnummer = 667, Durchwahl = 1234. Bei einem kommenden Anruf von 6671234 wird im Display 023026671234 angezeigt. Standardwert: Deaktiviert
Leitungswechsel bei Direktruf	Mit diesem Flag wird das Verhalten einer Direktruftaste definiert, wenn eine aktive Gesprächsverbindung auf einer MULAP-Leitung vorliegt. Relevant für Teamschaltung / Team-Gruppe, Chef/Sekretär / Top-Gruppe, Basic-MULAP, Chef-MULAP. Nach dem Drücken einer Direktruftaste wird ein Leitungswechsel durchgeführt. Das Gespräch wird gehalten und kann nur an diesem Telefon wieder aufgenommen werden. Standardwert: Deaktiviert (nicht für USA, Kanada), Aktiviert (nur für USA, Kanada)
Automatische Wahlwiederholung	Im Fall eines besetzten Teilnehmers wird eine automatische Wahlwiederholung durchgeführt. Über den Zeitparameter Zeit für automatische Wahlwiederholung wird definiert, nach welcher Zeit die Wahlwiederholung aktiv wird. Standardwert: Deaktiviert
Knoten-Rufnummer bei Voice Mail	Bei aktiviertem Flag wird bei vernetzten Kommunikationssystemen definiert, ob die Knoten-Rufnummer bei der Identifizierung eines zentralen oder mehrerer dezentraler Voice-Mail-Server mitzuliefern ist. Die Knoten-Rufnummer muss für die Identifizierung des oder der VoiceMail-Server mitgeliefert werden. Standardwert: Deaktiviert
Anrufübernahme nach Wiederanruf	Bei aktiviertem Flag werden Wiederanrufe und Rückrufe auch bei den anderen Mitgliedern einer Anrufübernahmegruppe signalisiert und können von diesen übernommen werden. Standardwert: Deaktiviert
Einstellbare CLIP	Bei aktiviertem Flag wird Anstelle der eigentlichen Rufnummer die unter Clip/Lin eingetragene Nummer zum gerufenen externen Anschluss übermittelt und am Display angezeigt. Bei leerem Eintrag Clip/Lin wird die Rufnummer übermittelt. Standardwert: Aktiviert

Parameter	Beschreibung
Anruferliste beim Zielteilnehmer im Falle Umleitung MULAP	Bei aktiviertem Flag werden bei einer Umleitung MULAP kommende Anrufe in der Anruferliste des Zielteilnehmers eingetragen. Standardwert: Deaktiviert
Rufweiterschaltung nach Deflect call / Single step transfer	Bei aktiviertem Flag gilt: Hat ein Teilnehmer eine Anrufumleitung zu einem externen Ziel aktiviert (Deflect Call), wird der Anruf bei diesem Ziel signalisiert. Nach abgelaufener Rufweiterschaltungszeit wird der Anruf bei einem in der Rufzielliste eingetragenen ersten Ziel und anschließend bei einem eventuell eingetragenen zweiten Ziel signalisiert. Beispiel: Für Teilnehmer A wurde ein Deflect Call auf Teilnehmer B ausgeführt, der in seiner Rufzielliste als erstes Ziel Teilnehmer C und als zweites Ziel Teilnehmer D eingetragen hat. Der Anruf wird bei Teilnehmer C und nach abgelaufener Rufweiterschaltungszeit bei Teilnehmer D signalisiert. Die Aktivierung dieses Flags ist nur sinnvoll, wenn auch das Flag Ermittlung des Ziels über Rufzielliste beim Deflect Call / Single Step Transfer aktiviert wird. Standardwert: Aktiviert
Ermittlung des Ziels über Rufzielliste beim Deflect call / Single step transfer	Bei aktiviertem Flag gilt: Hat ein Teilnehmer eine Anrufumleitung zu einem externen Ziel aktiviert (Deflect Call) wird der Anruf bei diesem Ziel signalisiert und nach abgelaufener Rufweiterschaltungszeit bei einem in der Rufzielliste eingetragenen weiteren Ziel. Beispiel: Für Teilnehmer A wurde ein Deflect Call auf Teilnehmer B ausgeführt, der in seiner Rufzielliste als erstes Ziel Teilnehmer C eingetragen hat. Der Anruf wird nach abgelaufener Rufweiterschaltungszeit bei Teilnehmer C signalisiert. Standardwert: Aktiviert
Hinweiston während Sprachaufzeichnung	Bei aktiviertem Flag gilt: Standardwert: Dektiviert
A-Rufnummer in AUN-Gruppen / Rufzuschaltung / Umleitungziel / RWS-Ziel	Bei aktiviertem Flag werden ob Rufnummer und Name eines Anrufers bei allen Mitgliedern einer Anrufübernahmegruppe, bei zugeschalteten Teilnehmern (Rufzuschaltung) und bei Umleitungs- und Rufweiterschaltungszielen angezeigt. Rufnummer und Name werden im Display angezeigt. Standardwert: Aktiviert
SPE Unterstützung	Bei aktiviertem Flag wird das Leistungsmerkmal Signaling and Payload Encryption SPE unterstützt. Die VoIP-Nutz- und Signalisierungsdatenströme vom und zum Kommunikationssystem und zwischen OpenStage-Systemtelefonen werden verschlüsselt. Standardwert: Deaktiviert
SPE Advisory Ton	Bei aktiviertem Flag gilt: Bei aktiviertem System-Flag SPE Unterstützung und Verwendung eines OpenStage-Telefons 15, 20, 20 E oder 20 G wird ein Teilnehmer, zusätzlich zur Displayanzeige, durch einen Hinweiston auf eine unverschlüsselte Verbindung hingewiesen. Das Einschalten des Teilnehmer-Parameters Payload Security ist Voraussetzung für die Nutzung von SPE durch einen Teilnehmer. Bei Verwendung eines OpenStage-Telefons 40, 40 G, 60, 60 G, 80 oder 80 G ist kein Hinweiston zu hören. Der Zustand der Verbindung (verschlüsselt/unverschlüsselt) wird dauerhaft im Display angezeigt. Standardwert: Deaktiviert

Parameter	Beschreibung
SIP-Prov. zu SIP Prov. transit	Bei aktiviertem Flag sind Transit-Leitungsverbindungen bei ITSP-Anschaltungen erlaubt. Eine Transit-Leitungsverbindung liegt vor, wenn ein Anruf zwei Leitungen desselben Kommunikationssystems belegt. Beispiel: Ein externer Anruf wird über einen ITSP an einen internen Teilnehmer geleitet. Der interne Teilnehmer übergibt dann den Anruf wieder über einen ITSP an ein externes Ziel. Dadurch entsteht eine Transit-Leitungsverbindung innerhalb des Kommunikationssystems. Für die Dauer des Anrufs werden zwei Leitungen belegt. Die sich ergebenden Transit-Leitungsverbindungen werden zugelassen. Standardwert: Deaktiviert
Wahl von * und # auf Leitungsschnittstellen	Bei aktiviertem Flag ist das Aktivieren und Deaktivieren von Centrex-Leistungsmerkmalen über IP-Leitungen (ITSP) und ISDN-Amtsleitungen möglich. Verschiedene Provider stellen Centrex (Central Office Exchange)-Leistungsmerkmale zur Verfügung, die anhand von Kennzahlen aktiviert und deaktiviert werden können. Die Eingabe einer Kennzahl muss im Wahlzustand erfolgen (zum Beispiel nach Eingabe der Leitungskennzahl). Die Eingabe beginnt immer mit * (Stern) oder # (Raute). Anschließend ist die eigentliche Kennzahl (Ziffern 0 bis 9) einzugeben und durch # (Raute) abzuschließen. Im Gesprächszustand ist das Aktivieren oder Deaktivieren von Centrex-Leistungsmerkmalen nicht möglich. Das Aktivieren und Deaktivieren von Centrex-Leistungsmerkmalen über IP-Leitungen (ITSP) und ISDN-Amtsleitungen ist möglich. Standardwert: Deaktiviert
Richtungskennzahl für MEX hinzufügen	Gilt nur für externe Anrufe, die über das ITSP Leistungsmerkmal "Mobile Extension (MEX)" eingeleitet werden. Bei aktiviertem Flag fügt das System für extern gehende Rufe automatisch die Amtskennziffer zur Rufnummer hinzu, wenn die Rufnummer aus mehr als 7 Ziffern besteht, da das System diese als externe Rufnummer interpretiert. Besteht die Rufnummer aus weniger als 7 Ziffern, wird die Amtskennziffer nicht hinzugefügt, da das System die Rufnummer als interne Rufnummer interpretiert. Ist das Flag deaktiviert, dann muss der Service Provider für alle extern gehenden Rufe die Amtskennziffer der Rufnummer hinzufügen. Standardwert: Deaktiviert
CMI MWI Hinweiston	Bei aktiviertem Flag ist der Hinweiston der Message Waiting Indication (MWI) für DECT-Telefone aktiviert (CMI: Cordless Multicell Integration). Bei neuen Nachrichten auf der Voice-Mailbox wird ein Hinweiston gesendet. Standardwert: Deaktiviert
offene Nummerierung	
aktiv	Bei offener Nummerierung, wird ein Teilnehmer identifiziert durch die Knotenrufnummer, gefolgt von seiner Rufnummer oder Durchwahlnummer. Dadurch können Teilnehmern in unterschiedlichen Knoten die gleiche Rufnummer vergeben werden. In einem vernetzten System steht dieses Flag immer für alle Anlagen gleich. Standardwert: Deaktiviert
Knoten-Rufnummer	Bei offener Nummerierung ist hier die Knotenrufnummer einzutragen. Ein Teilnehmer kann aus anderen Knoten nur erreicht werden durch Wahl dieser Knotenrufnummer gefolgt von der Teilnehmerrufnummer. Wenn die Summe der Ziffern der Knotenrufnummer und Teilnehmerrufnummer mehr als 7 Zeichen beträgt, wird eine entsprechende Warnung angezeigt. Standardwert: Deaktiviert
Transiterlaubnis	

Parameter	Beschreibung
Leistungsmerkmal Transit	Bei aktiviertem Flag sind Transitverbindungen erlaubt, die an bestimmte Leistungsmerkmale geknüpft sind, wie zum Beispiel externe Anrufumleitung, Übergeben und DISA-Anwendungen. Das ist unabhängig davon, ob es sich um Quer- oder Amt-zu-Amt-Verbindungen handelt. Standardwert: Aktiviert
Transit Durchwahl Quer	Bei aktiviertem Flag sind Transitverbindungen in Durchwahl bei Querverbindungen (vernetzte Kommunikationssysteme) erlaubt. Standardwert: Aktiviert
Transit Durchwahl Amt	Bei aktiviertem Flag sind Transitverbindungen in Durchwahl bei Amt-zu-Amt-Verbindungen erlaubt. Standardwert: Deaktiviert
Schalter Spezial	
CALL PROC nicht senden	Dieses Flag muss aktiviert werden, wenn der Service Provider keine Call Proceeding Messages (ISDN Message) vom Kommunikationssystem bekommen soll. Standardwert: Deaktiviert
Autom. zykl. Leitungsbelegung	Bei aktiviertem Flag belegen gehende Rufe bei fehlerhaftem Verbindungsaufbau (z. B. keine ACK-Quittung) zyklisch neue ISDN-Amtsleitungen. Leitungsnummern oder Richtungsnummern werden hochgezählt. Standardwert: Aktiviert
Einschränkung für UC-Anrufe	
Einschränkung für UC-Anrufe	Bei aktiviertem Flag werden alle vom System eingeleiteten UC-Anrufe (z. B. über den CallMe-Dienst) vor der Wahl geprüft, ob der anfordernde UC Benutzer die Berechtigung für diesen Anruf hat. Fehlt dem UC Benutzer die Berechtigung, wird der Anruf nicht ausgeführt. Standardwert: Deaktiviert

27.3.1.2 Grundeinstellungen > System > Zeitparameter

In der Tabelle werden alle einstellbaren Zeitparameter aufgelistet (Spalte **Beschreibung**). Über die Spalten **Basis** und **Faktor** kann der Timer-Wert für den jeweiligen Zeitparameter eingestellt werden. Dabei ist die Zeit = Basis x Faktor. Wird in der Spalte **Faktor** der Wert 255 eingetragen, dann wird dieser Timer unwirksam.

Parameterbeschreibung der Registerkarten:

- **Zeitparameter ändern**

Parameter	Beschreibung
NoFe Nachwahlzeit Code Empfänger Anschaltzeit	Steuert die Dauer der Anschaltung der Codeempfänger bei MFV-Endgeräten und damit die Wahlaufnahmebereitschaft. Nach Ablauf dieses Zeitgliedes wird der Code-Empfänger freigegeben. Wertebereich: 5 - 15 s
Zeit für das Aktivieren von Leistungsmerkmalen NoFe	Wird aktiviert, wenn an einem Endgerät die Signaltaste betätigt wird. Sie dient zur Unterscheidung, ob ein Teilnehmer eine Rückfrage zurücknehmen will oder ein Leistungsmerkmal wie z.B. Konferenz aktivieren will. Wertebereich: 2 - 4 s
Wiederbelegungssperrzeit	Wird bei Leitungssätzen gestartet und verhindert eine sofortige gehende Belegung nach dem Auslösen während dieser Zeit. Wertebereich: 0 - 5 s
Rückrufverzögerungszeit	Wird gestartet, wenn ein Endgerät nach Ruhe wechselt. Nach Ablauf dieser Zeit wird geprüft, ob ein automatischer Rückruf auszuführen ist. Damit hat der Teilnehmer die Gelegenheit weitere gehende Gespräche zu führen. Wertebereich: 0 - 60 s
Dauer des Rückrufes	Wird ein automatischer Rückruf nicht innerhalb dieser Zeit beantwortet, so wird der Ruf beendet, und der Rückruf vertagt. Wertebereich: 15 - 60 s
Abwurfzeit für Wiederanruf	Wird ein Wiederanruf eines vor dem Melden übergebenen Gespräches nicht innerhalb dieser Zeit beantwortet, so erfolgt der Abwurf zum Vermittlungsplatz, falls dieses Abwurfkriterium ausgewählt wurde. Wertebereich: 20 - 600 s
Rufzeit während Übergeben vor Melden	Wird ein vor dem Melden (auf besetzten Teilnehmer) übergebenes Gespräch nicht innerhalb dieser Zeit beantwortet, so erfolgt der Wiederanruf bei der Nebenstelle, die das Gespräch übergeben hat. Wertebereich: 30 - 600 s
Wahlende bei unvollständiger Wahl (Österreich)	Überwachungstimer für Durchwahl. Erfolgt innerhalb dieser Zeit keine Wahl, so wird die Durchwahl als unvollständig bzw. als keine Wahl erkannt. (Gilt nur für Österreich). Wertebereich: 10 - 30 s
Wahlendezeit (keine Wahl)	Wird die Wahl nicht innerhalb einer bestimmten Zeit begonnen, so wird automatisch ein Wahlende erzeugt. Wertebereich: 5 - 15 s
Zeit zwischen 1. und 2. Ansage bei FDW	Fax/DuWa, analoge Durchwahl, Zeit nach Sprachansage. Standardwert: 15 s
Zeit für Parken + Übergang halten	Die Reaktivierung des geparkten Gesprächs muss innerhalb eines Timeouts erfolgen. Wird das geparkte Gespräch nicht innerhalb dieser bestimmten Zeit abgefragt (wiederaufgenommen), erfolgt ein automatischer Wiederanruf zu der Station, die das Gespräch geparkt hat. Mit dem Wiederanruf verlässt das Gespräch den Haltezustand und geht in einen Ruf über. Wertebereich: 60 - 255 s

Parameter	Beschreibung
Wahlende bei unvollständiger Wahl	Wird die Wahl nicht innerhalb einer bestimmten Zeit fortgesetzt, so wird automatisch ein Wahlende erzeugt. Wertebereich: 10 - 20 s
NoFe Flashzeit Minimum	Zur Erkennung eines Flash-Zeichens wird eine Mindestzeit festgelegt, in der die Schleife unterbrochen sein muss. Standardwert: 0 s
NoFe Flashzeit Maximum	Zur Erkennung eines Flash-Zeichens wird eine Maximalzeit festgelegt, in der die Schleife unterbrochen sein darf. Standardwert: 0 s
Zeit für das Auslösen eines Wiederanrufes am VPL	Wird ein Wiederanruf am Vermittlungsplatz nicht innerhalb dieser Zeit angenommen, erfolgt Auslösen der Verbindung. Wertebereich: 30 - 180 s
HKZ NSA-Vorhaltezeit	Vorhaltezeit für Nummernschalter-Arbeitskontakt, dient zur Vermeidung von Wählgeräuschen im Hörer bei IWV-Apparaten (vor dem Impuls). Standardwert: 0 s
HKZ NSA-Nachhaltezeit	Nachhaltezeit für Nummernschalter-Arbeitskontakt, dient zur Vermeidung von Wählgeräuschen im Hörer bei IWV-Apparaten (nach dem Impuls). Standardwert: 0 s
Störausblendezeit für Ruf	Zeit zum Ausblenden von Leitungsstörungen bei IWV-Wahl. Standardwert: 0 s
Wahlende bei 1A Wahl	Gibt die Zeit an, nach der die letzte Ziffer beim 1A-Verfahren ausgewählt wird. Die Ausgabe einer Ziffer erfolgt nach Eingabe der nächsten Ziffer, die letzte Ziffer wird nach Ablauf des Timers ausgegeben oder vom Teilnehmer mit dem Wahlendekennzeichen # gekennzeichnet. Wertebereich: 4 - 4,5 s
Gebührennachlaufzeit	Wird eine Leitung ausgelöst, so können während dieser Zeit eintreffende Gebühreninformationen (Gebührenimpulse) auf analogen Leitungen vom Kommunikationssystem ausgewertet werden. Die Leitung ist während dieser Zeit für gehende Verbindungen gesperrt. Standardwert: 0 s
Zwischenwahlzeit bei IWV	Erlaubte Pause zwischen einzelnen Ziffern bei IWV. Standardwert: 10 s
Wähltonüberwachungszeit	Gibt die Zeitspanne an, wie lange bei belegen eines Trunks mit Wählton auf diesen Ton maximal gewartet werden soll. Läuft dieser Timer ab, so liegt eine Störung dieser Amtsleitung vor und der Satz geht in Störung. Standardwert: 10 s
Pausenzeit für IWV	Die IWV-Wahl erfolgt mittels Impuls-Pausen-Folgen, Erkennung von Pausen auf IWV-Leitungen. Standardwert: 0 s

Parameter	Beschreibung
Impulszeit für IWV	Die IWV-Wahl erfolgt mittels Impuls-Pausen-Folgen. Erkennung von Impulsen auf IWV-Leitungen. Standardwert: 0 s
Flashzeit für PABX	Unterbrechungszeit für Teilnehmerschleife zum Auslösen von Steuerfunktionen (z. B. Rückfrage) in der Anlage. Standardwert: 0 s
Flashzeit für Amtsbetrieb	Unterbrechungszeit für Teilnehmerschleife zum Auslösen von Steuerfunktionen (z. B. Rückfrage) auf der HKZ-Leitung. Standardwert: 0 s
Minimale Impulszeit bei IWV-NoFe	Die IWV-Wahl erfolgt mittels Impuls-Pausen-Folgen. Erkennung von Impulsen vom IWV-Telefon. Standardwert: 0 s
Maximale Impulszeit bei IWV-NoFe	Die IWV-Wahl erfolgt mittels Impuls-Pausen-Folgen. Erkennung von Impulsen vom IWV-Telefon. Standardwert: 80 ms
Sendezeit für MFV-Zeichen	Länderabhängige Dauer von MFV-Wahlzeichen. Standardwert: 80 ms
Pausenzeit zwischen MFV-Zeichen	Länderabhängige Pause zwischen MFV-Wahlzeichen. Standardwert: 80 ms
MOH Verzögerungstimer	Wird eine Verbindung gehalten, so wird MOH geschaltet, sofern dies konfiguriert wurde. Das Einschalten der MOH erfolgt jedoch erst nach Ablauf dieser Zeit, damit insbesondere beim Einleiten von Leistungsmerkmalen wie z.B. Konferenz keine MOH eingeschaltet wird. Wertebereich: 0 - 5 s
Pausenzeit vor Wahl (nur für Entwicklung)	Ist bei analogen Amtsleitungen keine Hörzeichenüberwachung möglich oder erwünscht, kann die Wahl automatisch nach dieser Zeit gestartet werden. Standardwert: 3 s
Gebührenpause in Min	Zeit zwischen Gebührenimpulsen. Standardwert: 0 min.
Gebührenimpuls in Min	Dauer von Gebührenimpulsen. Standardwert: 0 min.
NSA Meldepulszeit	Nummernschalter-Arbeitskontakt (IWV-Leitungen). Standardwert: 0 s
NSA Belegungspulszeit	Nummernschalter-Arbeitskontakt (IWV-Leitungen). Standardwert: 0 s
Auslösen falls keine Wahl erfolgt	Erfolgt eine Leitungsbelegung und innerhalb einer bestimmten Zeit keine Wahl, so wird die Verbindung ausgelöst. Der anfordernde Teilnehmer bekommt Besetztton signalisiert. Wertebereich: 5 - 30 s

Parameter	Beschreibung
IWV NoFe Minimale Zwischenwahlzeit	Zeit zwischen Wahlziffern bei IWV-Telefonen. Standardwert: 0 ms
MFV NoFe Flash Entprellzeit	Verhindert Mehrfach-Erkennung von Flash-Tastendruck. Standardwert: 0 ms
MFV-Beruhigungszeit Zeit	Wartezeit zur Vermeidung von Störungen von DTMF-Zeichen auf abgehenden Leitungen. Standardwert 100 ms
Flash-Beruhigungszeit (siehe Hilfe)	Wartezeit nach Flash auf analogen Leitungen. Standardwert: 1 s
Zykluslänge für Wiederinbetriebnahme	Zeit für Restart von analogen Leitungen, nachdem kein Wählton erkannt wurde. Standardwert: 120 s
Wahlpausenlänge	Gibt die Pausenzeit an, welche zwischen zwei Ziffern eingehalten werden soll, wenn ein Pausenkennzeichen erkannt wird. Wertebereich: 1 - 5 s
Störausblendezeit für Ruf bei PABX-Betrieb	Zeit zum Ausblenden von Leitungsstörungen. Standardwert: 0 s
Künstliches Wahlende	Bei Externwahl werden nach dem künstlichen Wahlende empfangene Ziffern als Rückfrage interpretiert. Wertebereich: 5 - 15 s
Zeit für automatische Wahlwiederholung	Nach Ablauf des Timers wird im Falle eines besetzten Teilnehmers eine automatische Wahlwiederholung durchgeführt. Voraussetzung dafür ist die Auswahl der Option Automatische Wahlwiederholung unter Flags. Wertebereich: 10 - 650 s
Störausblendung für den ersten Polaritätswechsel (FRK/SPA)	Zeit zum Ausblenden von Leitungsstörungen. Standardwert: 0 ms
Verzögerungszeit bis zur Ansage vor Melden	Stellt die Verzögerungszeit ein, nach der sich das Ansagegerät meldet. Wertebereich: 1,5 - 30 s
Zeit zwischen HT-Auswertung und der Wahl Trunk-HKZ	Legt die Zeit zwischen der Hörzeichenerkennung und der Wahl der ersten Ziffer über HKZ ins Amt fest. Wertebereich: 0 - 2 s
Die Pausenl. nach der Wahl des 2.AKZ	Legt die Pause fest, welche nach der Wahl des 2. Amtskennzeichens oder der Internationalen Kennzahl eingelegt wird. Übergang zum nächsten Vermittlungsknoten. Wertebereich: 1 - 5 s

Parameter	Beschreibung
Zeit bis zum Aufmerksamkeitston bei HKZ-Transit-Verbindungen	Transit-Verbindungen werden in Abhängigkeit der verwendeten Satztypen zeitlich überwacht. Dies erfolgt mit dem Ziel, dass eine Verbindung nicht unendlich lange bestehen bleibt. Wenn mindestens ein Satztyp dieser Transit-Verbindung über eine Auslöse-Erkennung verfügt, erfolgt in der Regel keine zeitliche Überwachung (Ausnahme siehe unten stehende Tabelle). Bei dem Satztyp HKZ gibt es keine Auslöseerkennung. Es gibt jedoch eine HW-Option für Silent Reversal. Damit wird eine Auslöseerkennung bei HKZ möglich. Die Tabelle für Transitüberwachung (für die US-spezifischen Satztypen gilt) zeigt für welche Satztypen eine Timer-Überwachung erfolgt. Die Dauer der Überwachung ist konfigurierbar. Bei der Verwendung von HKZ mit Silent Reversal ist jedoch zu beachten, dass es Rufnummern gibt, bei denen u. U. kein Melden erkannt wird, und damit auch kein Auslösen erkannt werden kann. Bei diesen Rufnummern handelt es sich in der Regel um Ansagedienste. Hier muss der Betreiber des Kommunikationssystems explizit drauf hingewiesen werden. Wertebereich: 120 s - 42 min
Zeit vom Aufmerksamkeitston bis zum Auslösen...	Erfolgt eine zeitliche Überwachung von Transit-Verbindungen, so erfolgt nach Ablauf des Überwachungstimers ein Aufmerksamkeitston. Damit das Gespräch beendet werden kann, wird die Verbindung nicht sofort getrennt, sondern erst nach Ablauf dieser Zeit. Wertebereich: 10 - 650
Auslösetimer für HKZ	Ein Ruf einer HKZ-Leitung über Durchwahl (DuWa) wird nach dieser Zeit ausgelöst, wenn kein Gespräch zustande kommt. Wertebereich: 30 s - 254 min
Nach Halten wird ein Aufmerksamkeitston geschaltet (Italien)	Nach Ablauf dieser Zeit erfolgt bei gehaltenen Verbindungen ein Anklopfen bei der haltenden Nebenstelle (ITL). Wertebereich: 30 - 180 s
LCR: Timer für künstliches Wahlende	Wartezeit nach der letzten Ziffer bis Wahlende angenommen wird (Blockwahl LCR). Standardwert: 5 s
Überwachung eines UCD-Rufes auf einer analogen Leitung (nur für Entwicklung)	Zeit für das Auslösen eines HKZ-Anrufes auf eine UCD-Gruppe, wenn es zu keinem Verbindungsaufbau gekommen ist. Wertebereich: 10 - 3810 s
Überwachung eines Übergeben vor Melden an eine UCD-Gruppe (nur für Entwicklung)	Erfolgt ein Übergeben vor Melden eines Gespräches auf eine UCD-Gruppe, so wird der Timer gestartet. Wird der übergebene Ruf nicht beantwortet, so erfolgt nach Timerablauf ein Wiederanruf. Wertebereich: 10 - 3810 s
Verzögerungs-Timer für PC-VPL	Zeit bis Update Message zum PC-Vermittlungsplatz (Business Attendant) gesendet wird. Wertebereich: 300 ms
USBS Timer Intervall	Für den Zugang über S0-Port, TA-S0, TA-RS232 und TA-API wird der User Signalling Bearer Service (USBS) auf Basis der ETS 300 716 verwendet. Wertebereich: 1 - 60 s
Timer für Toll Fraud Monitoring	Wird eine Verbindung in Transit geschaltet, so erfolgt nach Ablauf dieser Zeit eine Signalisierung am Display des Vermittlungsplatzes. Dieser kann dann ggf. einzelne Leitungen freischalten. Dies ist eine Möglichkeit um Transit-Verbindungen zeitlich zu überwachen. Wertebereich: 0 - 650 s

Parameter	Beschreibung
Sonderbesetztton wenn ZielTln. Ruf nicht annimmt	Nach Ablauf dieses Timers erhält der rufende Tln. den Sonderbesetztton, wenn der gerufene interne Tln. nicht abnimmt. Wertebereich: 30 - 120 s
Sonderbesetztton wenn Ltg. ohne Wahl belegt wird	Belegt ein Teilnehmer gehend eine Leitung und wählt anschließend nicht weiter, dann erhält er nach Ablauf des Zeitgliedes den Sonderbesetztton. Wertebereich: 20 - 60 s
Rufzeit übergeben vor Melden auf besetzten Tln.	Nach Ablauf dieses Timers wird ein Teilnehmer A, der von Tln. B zu einem besetzten Tln. C übergeben wurde, zurück auf Tln. B geleitet. Wertebereich: 15 - 180 s
Fehlersignalisierungs-Intervall	Mit der Fehlersignalisierungszeit wird ein Intervall mit dem Wertebereich von 1 Min. bis 15 Min. definiert. Kommastellen werden auf volle Minuten abgerundet, Werte kleiner als 1 Min. oder größer als 15 Min. werden als 15 Min. bewertet. Zyklisch werden nach Ablauf des Intervalls die aktuell im Event Log eingetragenen Class-B-Fehler an das Remote Center übermittelt. Wertebereich: 60 - 900 s

27.3.1.3 Grundeinstellungen > System > Display

Parameterbeschreibung der Registerkarten:

- **Display ändern**

Parameter	Beschreibung
Name/Rufnummer anzeigen	Es kann konfiguriert werden, welche der folgenden Daten bei Anrufen auf den Displays aller angeschlossenen Telefone angezeigt werden sollen: Nur Rufnummer, oder Name (falls vorhanden), oder Name und Rufnummer gleichzeitig. Wenn ein Telefon eine dieser Einstellungen nicht unterstützt, wird z. B. anstatt der gleichzeitigen Anzeige des Namens und der Rufnummer nur die Rufnummer angezeigt. OpenStage-Telefone sind für die gleichzeitige Anzeige des Namens und der Rufnummer geeignet. Standardwert: Name und Rufnummer
Übergeben vor Melden	Entweder wird bei Übergeben vor Melden die Rufnummer des Übergebenden oder die Rufnummer des Übergebenen angezeigt. Ein mit Übergeben vor Melden übergebenes Gespräch kann vom angerufenen Teilnehmer nicht abgewiesen werden. Bei Wahl von Übergebener wird am Display vor Zustandekommen der Verbindung und nach Auslösen der übergebende Teilnehmer angezeigt. Bei Wahl von Übergebender wird am Display der übergebende Teilnehmer angezeigt, solange dieser mit dem Empfangsteilnehmer verbunden ist. Nachdem der Übergebende aufgelegt hat und eine Verbindung zum Übergebenen besteht, springt das Display vom übergebenden zum übergebenen Teilnehmer um. Standardwert: Übergebener
Wiederanruf	Erfolgt nach Übergabe eines Anrufs ein Wiederanruf, kann beim Empfangsteilnehmer entweder die Nummer des Übergebenden oder die Nummer des Teilnehmers angezeigt werden, von dem der Wiederanruf ausgeht. Die Übergabe eines Gesprächs wird bei einem internen Teilnehmer B angezeigt. C bekommt bis zur Beantwortung durch B oder nach einem Wiederanruf durch A einen Rufton. Unter diesem Punkt kann konfiguriert werden, ob im Display des Übergabeziels B der Teilnehmer A (Anrufer) oder C (Übergeben-Ziel) angezeigt wird. Wird von Teilnehmer A ein Wiederanruf angenommen, so bekommen beide Teilnehmer meldet sich nicht im Display angezeigt. Standardwert: Übergeben-Ziel
Datum/Uhrzeit-Format	Das Datum kann in unterschiedlichen Formaten angezeigt werden. Standardwert: Europa - 24 Stunden-Format
Anruferliste, Modus	Bei Aktivierung von Interne und externe Rufe oder Nur externe Rufe werden alle nicht entgegengenommene Anrufe in einer Liste gespeichert, deren Inhalt dann später über eine Systemprozedur abgerufen werden kann. Bei Aktivierung von Externe Rufe und Gespräche werden auch angenommene Gespräche in der Anruferliste gespeichert. Es erfolgt kein Austragen einer Rufnummer aus der Anruferliste, weder bei kommenden noch bei gehenden Gesprächen. Wenn alle Speicherplätze der Anruferliste bereits vergeben sind, wird beim Speichern einer weiteren Rufnummer der älteste Eintrag überschrieben. Nicht angenommene Gespräche werden angezeigt, wie es bisher im Leistungsmerkmal Anruferliste beschrieben ist. Angenommene Gespräche werden so angezeigt, wie es über die Funktionalität der Anruferliste Rufnummer speichern üblich ist. Wird ein von extern kommender Anruf über den AutoAttendant an einen internen Teilnehmer vermittelt und der Teilnehmer ist gerade besetzt oder hat die Anrufumleitung aktiviert, erfolgt kein Eintrag in der Anruferliste. Standardwert: Nur externe Anrufe

Parameter	Beschreibung
Rufnummern-Unterdrückung	Bei aktiviertem Flag wird die Anzeige der Rufnummer im ISDN verhindert, d.h. der Gesprächspartner erhält keine Rufnummernanzeige (das Leistungsmerkmal muss auch bei der Telekom aktiviert sein). Bei Vernetzung mit weiteren Kommunikationssystemen wird der Name des Gesprächspartners ebenfalls nicht angezeigt. Es gibt Anrufszenarien, bei denen ein Anrufer über das Amt auf Präsentation eingeschränkt gesetzt wurde. Wenn dieses Flag aktiviert ist, wird die Rufnummer des Anrufers beim Angerufenen angezeigt. Wenn dieses Flag deaktiviert ist, wird der Text Rufnummer unbekannt angezeigt. Das Flag hängt immer von den Amtseinstellungen jedes Providers ab. Standardwert: deaktiviert
Telefonbuch	Teilnehmer können auf ein Online-Telefonbuch zugreifen, das die Namen und Teilnehmerrufnummer aller internen Nebenstellen enthält. An den systemspezifischen Display-Endgeräten gibt es die Möglichkeit, sich alle vorhandenen internen Teilnehmer mit Namen und Rufnummer anzusehen, gezielt zu suchen und anschließend den gewünschten Teilnehmer anzurufen. Bei Endgeräten mit alphanumerischer Tastatur kann diese zur gezielten Suche benutzt werden. Wählen Sie aus der Liste die entsprechende Option aus: nein: kein Zugriff auf das Telefonbuch möglich, intern: Zugriff auf das interne Telefonbuch (Teilnehmer, Gruppen und KWZ (Kurzwahlziele)) möglich, LDAP: Zugriff auf die Telefonbuchinformationen des LDAP-Servers. Der LDAP-Zugriff muss über LDAP eingerichtet sein. alle: Teilnehmer kann zwischen dem Zugriff auf das interne Telefonbuch oder LDAP-Telefonbuch wählen. Standardwert: Intern
Schalter	
Gesprächsdauer anzeigen	Bei gehenden externen Gesprächen werden keine Gebühreninformationen angezeigt. Bei UP0/E-Endgeräten mit Display wird dann die aktuelle Gesprächsdauer angezeigt. Der Startpunkt der Zeiterfassung wird bei analogen Leitungen über einen Timer gesetzt (5 s nach Wahlende), bei digitalen Amtsleitungen mit CONNECT. Bei S0-Endgeräten wird vom Kommunikationssystem keine Anzeige der Gesprächsdauer unterstützt. Standardwert: deaktiviert
DTMF verdeckte Anzeige	PIN-Code-Eingaben werden an Systemtelefonen mit Display verdeckt angezeigt. Standardwert: aktiviert
Displayanzeige bei Info-Meldung	Vorliegende Info-Meldungen werden am Display der Systemtelefone angezeigt. Standardwert: aktiviert
Rufnummer transparent weiterreichen	Im Falle einer Anrufumleitung oder Rufweiterschaltung zu einem externen Teilnehmer werden dem gerufenen Teilnehmer die Rufnummer des rufenden Teilnehmers angezeigt. In einem vernetzten System ist die Option in dem Knoten zu setzen, an dem ein Amtsanschluss angeschaltet ist. Voraussetzung für das Funktionieren des LM ist die freigeschaltete Clip-No-Screening-Funktion im Amt, die kostenpflichtig ist. Dieses Flag arbeitet wechselwirksam mit dem Flag TIn-RufNr unterdrücken unter Richtungen zusammen. Standardwert: deaktiviert

27.3.1.4 Grundeinstellungen > System > DISA

Parameterbeschreibung der Registerkarten:

- **Disa ändern**

Parameter	Beschreibung
DISA	
Durchwahl	Rufnummer, unter der die DISA-Funktion von extern erreicht werden kann. Die Rufnummer kann für externe und interne Nutzung unterschiedlich sein.
Sicherheits Modus	Um die DISA-Funktionen nutzen zu können, muss der Teilnehmer ein Kennwort eingeben. Über die Optionen im Sicherheitsmodus kann festgelegt werden, ob der Teilnehmer nach Eingabe des Kennworts zunächst warten muss oder ob er # (Raute) eingeben muss. Standardwert: Nach Zeit
DISA intern	
Rufnummer	DISA Intern bezieht sich auf die Nutzung an einem anderen, mittels IP-vernetzten Knoten.
Mobility Callback	
Durchwahl	Die Authentifizierung mittels Passwort entfällt, wenn ein als Mobility-Rufnummer erkannter Anruf von extern auf die DISA-Durchwahlnummer erfolgt. In diesem Fall wird direkt der interne Wählton angeschaltet. Hierfür muss das Endgerät des externen Teilnehmers seine Rufnummer übermitteln. Diese Rufnummer wird dann gegen die Mobility-Liste geprüft.

27.3.1.5 Grundeinstellungen > System > Abwurf/VPL/Hotline

Parameterbeschreibung der Registerkarten:

- **Abwurf/VPL/Hotline ändern**

Parameter	Beschreibung
Abwurfplatz	
Tag/Nacht	Rufnummer des Abwurfplatzes. Der Abwurfplatz kann für Tag und Nacht getrennt festgelegt werden. Darüber hinaus besteht die Möglichkeit, bei der Aktivierung der Nachtschaltung auch ein beliebiges Ziel anzugeben (variable Nachtschaltung).
Zentraler Abwurfplatz	
Richtung	Richtungsindex für den zentralen Abwurfplatz bei vernetzten Kommunikationssystemen
Rufnummer	Rufnummer des zentralen Abwurfplatzes bei vernetzten Kommunikationssystemen
Abwurf zum Abwurfplatz	
im Freifall	Der Ruf folgt der festgelegten Prozedur für Kommende Rufe. Ist das Ende der Tabelle erreicht, so wird geprüft, ob Abwurf nach Zeit erfolgen soll oder nicht. Gegebenenfalls wird nach der unter Rufweiterschaltung festgelegten Anzahl von Ruftönen der Abwurfplatz gerufen. Aus einem Sammelanschluss erfolgt kein Abwurf. Der Ruf wird wieder zum ersten Sammelanschluss-Teilnehmer weitergeschaltet und verbleibt stetig im Sammelanschluss. Standardwert: aktiviert

Parameter	Beschreibung
im Besetztfall	Im Besetztfall wird zunächst geprüft, ob angeklopft werden kann oder nicht. Wenn nicht angeklopft werden darf (Anklopfschutz oder Abwurfkriterium), so folgt der Ruf dem Call Management/Anrufrouting. Kann der Ruf bei keinem Teilnehmer signalisiert werden, so wird geprüft, ob Abwurf erfolgt oder ausgelöst wird (B-Signalisierung ins Amt). Ist ein analoger Fernsprecher mit Anklopfschutz besetzt, so wird bei allen Satztypen ausgelöst. Bei MFV-Durchwahl und bei HKZ erfolgt immer Abwurf. Standardwert: deaktivert
bei Falschwahl	Wenn eine falsche Rufnummer gewählt wird, wird geprüft, ob Abwurf erfolgen soll. Bei MFV-Durchwahl erfolgt immer Abwurf. Standardwert: aktiviert
bei unvollständiger Wahl	Wenn die gewählte Teilnehmerrufnummer nicht vollständig ist, wird nach Ablauf der voreingestellten Zeit der Abwurfplatz gerufen. Die Zeit kann im Feld Wahlende bei unvollständiger Wahl unter Zeitparameter eingestellt werden. Standardwert: aktiviert
bei nicht beantwortetem Wiederanruf	Wird ein externer Anruf nach Übergeben vor Melden von Teilnehmer A auf Teilnehmer B von Teilnehmer B nicht abgefragt und erfolgt nach Wiederanruf auf Teilnehmer A ebenfalls kein Melden, so wird nach Ablauf der voreingestellten Zeit der Abwurfplatz gerufen. Die Zeit kann im Feld Wahlende bei unvollständiger Wahl unter Zeitparameter eingestellt werden. Wenn das Flag nicht aktiviert ist, wird nach Ablauf der eingestellten Zeit das Gespräch ausgelöst. Standardwert: deaktivert
bei Ablehnung	Falls ein interner Teilnehmer den Anruf mit "Ruf abweisen" ablehnt, so folgt der Ruf dem Call Management/Anrufrouting. Kann der Ruf bei keinem Teilnehmer signalisiert werden, so wird geprüft, ob Abwurf erfolgt oder ausgelöst wird (B-Signalisierung ins Amt). Standardwert: aktivert
Abwurf bei Codeschloss	
Rufnummer	Wenn bei einem Teilnehmer das Codeschloss aktiviert ist und es wird von diesem Teilnehmer eine Bündelkennzahl gewählt, wird der Anruf unverzüglich zum eingetragenen Abwurfziel umgeleitet. Somit wird ein Anruf bei Wahl einer Nummer, für die der Teilnehmer keine Berechtigung hat, bei der angegebenen Teilnehmerrufnummer signalisiert. Die Funktion Abwurf bei Codeschloss lässt sich individuell für jeden Teilnehmer über die Teilnehmerflags einstellen.
Platzkennzahl	
Rufnummer intern	Über diese Rufnummer kann der Abwurfplatz von internen Geräten aus erreicht werden. Nach Änderung der internen Rufnummer des Vermittlungsplatzes, wird ein Download zur IVM automatisch angestoßen. Wertebereich: Freie Eingabe einer Ziffer, sofern nicht bereits im Rufnummernplan belegt
Rufnummer extern	Über diese Rufnummer wird der Abwurfplatz in Durchwahl oder aus dem Anlagennetz (CorNet-N bzw. CorNet-NQ) erreicht.
Hotline	
Röchel-Zeit	Wenn ein Teilnehmer den Telefonhörer abnimmt, dann wird nach Ablauf der Röchel-Zeit die Hotline automatisch gerufen, allerdings nur, wenn innerhalb dieser Zeit vom Teilnehmer keine Ziffer eingegeben wird. Die Röchel-Zeit wird in Sekunden angegeben.

Parameter	Beschreibung
Ziel-Ruf-Nr. 1 bis 6	Systemweit können 6 Hotline-Ziele eingetragen werden, die Auswahl erfolgt je Teilnehmer (siehe Teilnehmer/Teilnehmer-Parameter ändern)
Vermittlungsplatz	
Wartende Anrufe	Hier kann die Anzahl der maximal wartenden Anrufe ausgewählt werden. Erreicht die Anzahl der Teilnehmer in der Warteschlange des Vermittlungsplatzes diesen numerischen Wert, so erfolgt eine Rufweiterschaltung zu einem konfigurierbaren Überlaufziel. Wertebereich: 1-15
Wartezeit	Hier kann eine Wartezeit in Sekunden eingegeben werden. Nach Überschreitung dieser Zeit erfolgt eine Rufweiterschaltung zu einem über das Call Management festgelegten Überlaufziel.
Schnellvermitteln	Ist dieses Flag gesetzt, kann die Vermittlung einen Anruf durch Eingabe der entsprechenden Teilnehmerrufnummer an einen anderen Teilnehmer übergeben. Schnellvermitteln kann nur aktiviert werden, wenn das systemweite Flag **DTMF automatisch** ausgeschaltet ist. Standardwert: deaktivert
Unbewählt vermitteln	Ein berechtigter Teilnehmer (Vermittlungsplatz VPL) hat die Möglichkeit, einem internen Teilnehmer mit nicht ausreichender Amtsberechtigung eine unbewählte Amtsleitung zuzuteilen, um diesem Teilnehmer das Führen genau eines externen Gespräches zu ermöglichen. Nach der Übergabe der vermittelten Leitung an den nicht ausreichend berechtigten Teilnehmer erfolgt eine Wahlkontrolle anhand einer zusätzlichen Amtsberechtigung für vermittelte Leitungen. Nur wenn diese zusätzliche Amtsberechtigung ausreicht, d.h. wenn der Teilnehmer z.B. eine gültige Nummer gemäß Verbots-oder Erlaubnisliste für vermittelte Leitungen wählt, wird die gehende externe Verbindung zugelassen. Der Teilnehmer wählt auf einer vermittelten Leitung selbst die Belegungskennzahl. Es ist im Kommunikationssystem über einen Referenzteilnehmer eine Amtsberechtigung für vermittelte Leitungen pro Richtung konfigurierbar. Der Standard-Referenzteilnehmer ist der erste logische Teilnehmerport bzw. der Vermittlungsplatz. Die Standardberechtigung steht auf volle Amtsberechtigung für alle Richtungen. Standardwert: deaktivert
Sonstige Kriterien	
Anklopfen im Besetzfall	Ist dieses Flag aktiviert, ist bei sämtlichen Teilnehmern im Kommunikationssystem das Leistungsmerkmal "Anklopfen" aktiv ist. Standardwert: aktivert
Sonstiges Anklopfen durch VPL	Nur relevant in CorNet-vernetzten Systemen. Wenn das Flag gesetzt ist, kann nur ein rufender VPL (System A) beim Teilnehmer B (System B) anklopfen. Alle anderen Teilnehmer des System A können im System B nicht anklopfen. Für die Teilnehmer innerhalb des Systems B gilt die Bedingung des Anklopfschutzes (siehe Teilnehmersicht: Flags) für den jeweiligen Teilnehmer. Wenn das Flag nicht gesetzt ist, können alle Anrufe auf besetzte Teilnehmer in einem anderen System sofort anklopfen, wenn der Teilnehmer nicht Anklopfschutz aktiviert hat. Das Flag muss gesetzt werden, wenn erreicht werden soll, dass ein rufender VPL bei einem besetzten Teilnehmer sofort in den Wartezustand gesetzt wird und anklopfen kann. Wenn das Flag nicht gesetzt wird, dann bekommt der VPL den Besetztton und geht erst nach einigen Sekunden in den Wartezustand. Standardwert: deaktivert

Parameter	Beschreibung
Aufschalten durch VPL	Ist dieses Flag aktiviert, ist der Abwurfplatz für das Leistungsmerkmal "Aufschalten" berechtigt. Damit kann er sich in ein Gespräch eines internen Teilnehmers einschalten. Standardwert: aktivert
Substitution	
*	Kennziffer, die bei IWV-Normalfernsprechern und ISDN-Endgeräten * (Stern) ersetzen. Standardwert: 75
#	Kennziffer, die bei IWV-Normalfernsprechern und ISDN-Endgeräten # (Raute) ersetzen. Standardwert: 76

27.3.1.6 Grundeinstellungen > System > LDAP

Parameterbeschreibung der Registerkarten:

- **LDAP ändern**

Parameter	Beschreibung
LDAP-Zugang	
IP-Adresse des LDAP-Servers	IP-Adresse des LDAP-Servers, von dem die Telefonbuchinformation geholt werden soll.
Port-Nummer des LDAP-Zugangs	Port-Nummer für den LDAP-Zugang. Standardwert: 389
Benutzername/Kennwort	Unter Windows Server ADS ist ein Anonymus-Zugriff nicht möglich. In diesem Fall hier Benutzernamen und Kennwort für die LDAP-Anbindung eingeben. Wertebereich: max. 48 Zeichen
LDAP-Server-Parameter	
Basis DN	DN = Distinguished Name; Suchbasis für die Suchanfrage an den LDAP-Server (ASCII, 100 Zeichen), z. B. ou=com, cn=unify, cn=de
Suchanfrage	Muster für die Suchanfrage an den LDAP-Server. Als Platzhalter für den zu suchenden Namen muss das Zeichen $ eingegeben werden. Wertebereich: ASCII, 50 Zeichen Standardwert: cn=$*
Ergebnisattribut Name	Das Ergebnisattribut Name unterstützt Zeichen des Zeichensatzes ISO-8859-1 mit Codewerten im Bereich von 0x20 bis 0x80 (ASCII-Zeichen), sowie die Zeichen Ä, Å, Æ, Ñ, Õ, Ö, Ø, Ü, ß, ä, õ, ö, ü. Die Anzeige der Zeichen ist abhängig von der Spracheinstellung des Teilnehmers und dem verwendeten Endgerät. Wertebereich: ASCII, 24 Zeichen Standardwert: cn

Parameter	Beschreibung
Ergebnisattribut Rufnummer	Im Ergebnisattribut Rufnummer dürfen bis zu 25 Wahlziffern (0...9, *, #) und bis zu 6 Zeichen zur Formatierung (+,(), Leerzeichen, -) zurückgeliefert werden. Die Rufnummer muss im kanonischen Rufnummernformat vorliegen (z. B. +49 (89) 70070) Wertebereich: ASCII, 25 Zeichen Standardwert: telephoneNumber
Sortieren der Suchergebnisse	Die Suchergebnisse werden alphabetisch sortiert nach Name angezeigt. Standardwert: aktiviert
LDAP-Rufnummernauswertung	
LDAP-Belegungskennzahl	Die Belegungskennzahl entspricht der gewählten Richtungskennzahl. Standardwert: 0 (Default-Richtungskennzahl der ersten Richtung)
LDAP-Rufnummernprefix	Das hier angegebene Präfix wird der gefundenen Rufnummer vorangestellt. Wertebereich: ASCII, 5 Zeichen

27.3.1.7 Grundeinstellungen > System > Texts

Parameterbeschreibung der Registerkarten:

- **Texte ändern**

Parameter	Beschreibung
Zurücksetzen auf Default-Werte	Info- und Antwort-Texte auf die voreingestellten Werte einer bestimmten Sprache zurücksetzen. Die Rücksetzung erfolgt durch Auswahl der Sprache in der Aufklappliste.
Info-Texte	Kurznachrichten, die ein Teilnehmer an einen anderen Teilnehmer senden kann. Standardmäßig sind im Kommunikationssystem zehn solcher Texte vorkonfiguriert. Jeder dieser Standard-Texte kann überschrieben werden. Dabei sind allerdings immer nur zehn Meldungen verfügbar. Der Teilnehmer kann auf diese Info-Texte über den Menüpunkt Infos senden? am Systemtelefon zugreifen. Teilnehmer mit Endgeräten, die eine alphanumerische Tastatur haben, können darüber hinaus auch selbst Meldungen erstellen; allerdings können sie die Standard-Meldungen nicht ändern. Wertebereich: maximal 24 alphanumerische Zeichen
Antwort-Texte	Kurznachrichten, die der Teilnehmer einem Anrufer bei Abwesenheit zukommen lassen kann. Es stehen 10 Standard-Texte zur Verfügung. Jede dieser Standard-Meldungen kann überschrieben werden. Teilnehmer mit Endgeräten, die eine alphanumerische Tastatur haben, können darüber hinaus auch selbst Meldungen erstellen; allerdings können sie die Standard-Meldungen nicht ändern. Zumeist wird der Teilnehmer die bestehenden Meldungen nur um bestimmte Zusatzinformationen ergänzen wollen. Bei Texten mit einem Doppelpunkt hat der Teilnehmer die Möglichkeit, eine Nachricht, eine Nummer oder ein Datum zu ergänzen. Der Teilnehmer kann auf die Antwort-Texte über den Menüpunkt Hinweismeldung an? am Systemtelefonen zugreifen. Wertebereich: maximal 24 alphanumerische Zeichen

27.3.1.8 Grundeinstellungen > System > Flexible Menüs

Flexible Menüs ermöglichen die kundenindividuelle Anpassung der Menüpunkte im Servicemenü der Systemtelefone. Bei aktiviertem Kontrollkästchen in der **Ausblendliste** wird dieser Menüpunkt nicht angezeigt. Diese Einstellung gilt systemweit für alle Systemtelefone. Ausgeblendete Funktionen können weiterhin per Kennziffer aktiviert werden.

27.3.1.9 Grundeinstellungen > System > Kurzwahlziele

Es können bis zu 8000 Telefonbucheinträge manuell eingerichtet oder geändert werden. Bei den Kurzwahlzielen handelt es sich um zentrale Kurzwahlnummern (RNGZ). Durch Klicken auf einen Spaltennamen werden die Einträge in der entsprechenden Spalte sortiert.

Parameterbeschreibung der Registerkarten:

- **Kurzwahlziel ändern**

Parameter	Beschreibung
Kurzwahl	Nummer, die vom Teilnehmer gewählt wird. Die Kurzwahl-Nummern müssen vierstellig sein (`0000-7999`, führende Nullen verwenden).
Rufnummer	Wählbare Rufnummer der gewünschten Zielstelle, d. h. mit einer Richtungs- oder Leitungskennzahl (z. B. 0, 9, 81 oder 801). Wertebereich: max. 31 Ziffern
Name	Name für das Kurzwahlziel, wie er im internen Telefonbuch gespeichert und bei Anwahl des dazugehörigen Kurzwahlziels angezeigt werden soll. Kommende Rufe (mit CLIP) werden mit den gespeicherten Kurzwahlzielen verglichen und als Name des Kurzwahlziels angezeigt, wenn der Displayparameter Name bzw. Name und Rufnummer aktiviert ist. Wertebereich: max. 16 Zeichen
Suche	Wird in die Suchfelder **Kurzwahl**, **Rufnummer** oder **Name** ein Suchbegriff eingegeben und anschließend die Return-Taste gedrückt, werden alle Treffer angezeigt, die den Suchbegriff enthalten. Mit der Eingabe von `521` als Rufnummer werden z. B. die Treffer `+495213535` und `+498967521` angezeigt oder mit `co` als Name die Treffer `Collins`, `Mcoin` und `Branco`. Alle Einträge werden angezeigt, wenn in allen Suchfeldern nichts eingetragen ist und anschließend die Return-Taste gedrückt wird.
Schaltflächen	
Übernehmen	Neue Einträge hinzufügen oder vorhandene Einträge ändern.
Rückgängig	Änderungen für vorhandene Einträge zurücksetzen (vor Übernehmen).

Parameterbeschreibung der Registerkarten:

- **Textdatei (csv/xml) importieren/exportieren über HTTP**

Parameter	Beschreibung
CSV/XML-Datei über HTTP importieren	Kurzwahlziele können über eine XML- oder CSV-Datei im UTF-8-Format importiert werden. Bereits bestehende Kurzwahlnummern werden vor dem Import gelöscht. Eine XML- und eine CSV-Vorlage für den Import von Kurzwahlnummern findet sich unter **Service-Center > Dokumente > CSV Vorlagen.**
XML-Datei über HTTP exportieren	Kurzwahlziele können als XML-Datei im UTF-8-Format exportiert werden. Es werden immer alle Datensätze exportiert.

27.3.1.10 Grundeinstellungen > System > Servicekennzahlen

Ein Teilnehmer kann Leistungsmerkmale des Kommunikationssystems über sein Telefon über die Servicekennzahlen aktivieren und deaktivieren. Die Standard-Servicekennzahlen können geändert werden, wobei zu beachten ist, dass die Vergabe der Kennzahlen konsistent ist.

27.3.1.11 Grundeinstellungen > Gateway

Parameterbeschreibung der Registerkarten:

- **Gateway-Eigenschaften ändern**

Parameter	Beschreibung
Allgemein	
Kunden-Name	Frei wählbarer Name des Kunden, nur für Informationszwecke (optional) Wertebereich: max. 15 Stellen
Vertragsnummer	Frei wählbare Zeichenfolge, für Informationszwecke (optional) Wertebereich: unbegrenzt
System-Name	Frei wählbarer Name des Kommunikationssystems. Diese Zeichenfolge wird im Display aller Systemtelefone angezeigt. Wertebereich: max. 24 Stellen
Gateway-Standort	Frei wählbare Zeichenfolge zur Angabe des Aufstellungsorts des Kommunikationssystems. Diese Information hilft einem Servicetechniker, das Kommunikationssystem zu finden, wenn ein physischer Zugang zum Kommunikationssystem nötig ist. (optional) Wertebereich: unbegrenzt
Kontakt-Adresse	Frei wählbare Zeichenfolge zur Angabe einer Kontaktperson, die bei Problemen mit dem Kommunikationssystem angesprochen werden kann. (optional) Wertebereich: unbegrenzt
System-Länderkennzeichen	Auswahl des Landes, in dem das Kommunikationssystem betrieben wird; das Ändern des System-Länderkennzeichens erfordert einen Reboot, der automatisch durchgeführt wird.
Gateway-IP-Adresse	Anzeige der IP-Adresse des Kommunikationssystems, z.B. 192.168.1.2.

Parameter	Beschreibung
Gateway-Netzmaske	Anzeige der Netzmaske des Kommunikationssystems, z.B. 255.255.255.0.
Internationales Präfix	Angabe des Präfix für internationale Wahl, z.B. 00 für Deutschland oder 011 für USA.
Nationales Präfix	Angabe des Präfix für nationale Wahl, z.B. 0.
Produkt	Auswahl des erworbenen Produkts (OpenScape Business oder Octopus F X)
Gateway-Standort	
Ländervorwahl	Angabe der Ländervorwahl, z.B. 49 für Deutschland oder 1 für USA.
Ortsnetzkennzahl	Angabe der Ortsnetzkennzahl, z.B. 89 für München.
Anlagenrufnummer	Angabe der Anlagenrufnummer (Kopf-Nr. ohne Tln.-Durchwahl), z.B. 7007
Vernetzungsparameter	
Knoten-ID	Für jeden Knoten in einem vernetzen System muss eine eindeutige Knoten-ID vergeben werden. Damit sind die einzelnen Knoten in vernetzten Systemen eindeutig identifizierbar. Wertebereich: 1 bis 100
Interner Wählton	
Dauerton	Ist dieses Flag aktiviert, ist der interne Wählton keine Tonfolge sondern ein Dauerton. Der interne Wählton ertönt, sobald man den Telefonhörer abgenommen und noch keine Ziffer gewählt hat. Standard: deaktiviert

27.3.1.12 Grundeinstellungen > DynDNS > DynDNS Service

Parameterbeschreibung der Registerkarten:

- **DynDNS Konfiguration anzeigen**
- **DynDNS Konfiguration ändern**

Parameter	Beschreibung
DynDNS aktivieren	Mit Hilfe des DynDNS-Service kann von verschiedenen Orten auf das Kommunikationssystem zugegriffen werden, ohne dass die aktuelle IP-Adresse des Gateways bekannt sein muss. Der DynDNS-Service kann hier aktiviert werden.
Benutzerdefinierte Domäne	Kontrollkästchen muss aktiviert werden, wenn der DynDNS-Anbieter nicht in der Liste **Domainname** enthalten ist.
Benutzername	Benutzername des DynDNS-Accounts beim DynDNS-Anbieter. Das Einrichten von DynDNS-Accounts ist z. B. unter der Internet-Adresse `http://www.dyndns.org/account/create.html` möglich.
Passwort	Passwort des DynDNS-Accounts beim DynDNS-Anbieter. Bei der Eingabe werden aus Sicherheitsgründen nur Platzhalterzeichen angezeigt.
Passwort wiederholen	Wiederholung des Passworts des Benutzerkontos beim DynDNS-Service. Bei der Eingabe werden aus Sicherheitsgründen nur Platzhalterzeichen angezeigt.

Parameter	Beschreibung
Hostname	Eingabe des beim DynDNS-Anbieter registrierten Hostnamens ohne den Domainnamen, z.B. myhost. Der komplette Subdomain-Name setzt sich aus dem Hostnamen und dem Domainnamen zusammen, z.B. myhost.dyndns.org.
Domainname	Auswahl des DynDNS-Anbieters aus einer Liste (z.B. dyndns.org) oder manuelle Eingabe des DynDNS-Anbieters (falls Kontrollkästchen **Benutzerdefinierte Domäne** aktiviert ist).

Update-URL	Eingabe der Update-URL eines nicht in der Liste enthaltenen DynDNS-Anbieters. Der Aufbau dieser URL ist abhängig vom DynDNS-Anbieter. Zusätzlich sind kundenspezifische Parameter (im Beispiel *kursiv* markiert) zu ergänzen.
	Beispiel einer Update-URL:
	`http://www.anydns.info/update.php?user=<`*`username`*`>&password=<`*`pass`*`>&host=<`*`domain`*`>&ip=<`*`ipaddr`*`>`
	Beispiel einer Update-URL mit Base64 verschlüsselter Authentifizierung:
	`https://<b64><`*`username`*`>:<`*`pass`*`></b64>@members.dyndns.org/nic/update?hostname=<`*`domain`*`>&myip=<`*`ipaddr`*`>&wildcard=NOCHG&mx=NOCHG&backmx=NOCHG`
	<b64>...</b64> für Base64 codierte Parameter

Zuletzt aktualisiert	Zeitpunkt der letzten Aktualisierung beim DynDNS-Service.
IP-Adresse beim DynDNS	IP-Adresse beim DynDNS-Anbieter, auf die Anfragen für Ihre eingerichtete DynDNS-Subdomain geroutet werden.
Eigene dynamische IP-Adresse	Anzeige der aktuellen IP-Adresse des Kommunikationssystems, die vom Internet Service-Provider zugewiesen wurde.
Wildcard aktivieren	Wird diese Option aktiviert, werden Anfragen nach Sub-Subdomains wie beliebig.myhost.dyndns.org auf myhost.dyndns.org geroutet.
Mail Exchanger	Der Mail Exchanger (MX-Record) gibt innerhalb des DNS an, an welche IP-Adresse oder an welchen Domainnamen E-Mails für die eingerichtete DynDNS-Subdomain zu schicken sind. Hinter dem angegebenen Ziel muss sich ein Mailserver befinden.
Backup MX	Wird diese Option aktiviert, werden E-Mails, die nicht an den angegebenen Mail-Exchanger zugestellt werden können, weil dieser beispielsweise temporär nicht verfügbar ist, beim DynDNS-Service zwischengespeichert und zugestellt, wenn der eigene Mail Exchanger wieder verfügbar ist.
HTTPS für die Aktualisierung verwenden	Wird diese Option aktiviert, wird für die Aktualisierung die sichere verschlüsselte HTTPS-Verbindung gewählt.

27.3.1.13 Grundeinstellungen > DynDNS > Aktualisierungszeit der DNS-Namen

Parameterbeschreibung der Registerkarten:

- **Aktualisierungszeit ändern**

Parameter	Beschreibung
DNS-Namen aktualisieren	Diese Option gilt nur für VPN. Nach Ablauf der Zeit, die in „Timer-Wert für Aktualisierung der DNS-Namen“ eingestellt ist, überprüft die VPN-Komponente, ob sich eventuell verwendete DNS-Namen in der VPN Konfiguration zu neuen IP-Adressen auflösen (VPN mit dynamischen IP Adressen). In dem Fall wird VPN mit den neuen IP Adressen rekonfiguriert.
Timer-Wert für Aktualisierung der DNS-Namen (s)	Sekundenanzahl für das Intervall zwischen zwei Aktualisierungen. Wertebereich: 60 - 1800, Standardwert: 180

27.3.1.14 Grundeinstellungen > Quality of Service

Beim IP-Datenverkehr werden die IP-Pakete, die das Kommunikationssystem selbst generiert, in fünf Gruppen aufgeteilt. Für vier dieser Gruppen kann eingestellt werden, mit welchem Codepunkt die Pakete markiert werden sollen. Der übrige Datenverkehr wird nicht proirisiert (also 00 markiert).

Prioritätsklasse	ToS-Wert Binär	ToS-Wert Hexadezimal
AF (Assured Forwarding)		
AF11	001-010-00	28
AF12	001-100-00	30
AF13	001-110-00	38
AF21	010-010-00	48
AF22	010-100-00	50
AF23	010-110-00	58
AF31	011-010-00	68
AF32	011-100-00	70
AF33	011-110-00	78
AF41	100-010-00	88
AF42	100-100-00	90
AF43	100-110-00	98
EF (Expedited Forwarding)		
EF	101-110-00	B8
Best Effort (BE)		
BE	000-000-00	00
CS (Class Selector)		
CS3	011-000-00	60
CS4	100-000-00	80
CS5	101-000-00	A0

Prioritätsklasse	ToS-Wert Binär	ToS-Wert Hexadezimal
CS6	110-000-00	C0
CS7	111-000-00	E0
Manuelle Eingabe	xxx-xxx-00	0-63 (dezimal)

Parameterbeschreibung der Registerkarten:

- **Quality of Service ändern**

Parameter	Beschreibung
Prioritätsklasse für Signalisierungsdaten	Call Signaling für den Verbindungsaufbau bei H.323/SIP Standardwert: AF31
Prioritätsklasse für Fax/Modem-Payload	Data Payload, zum Beispiel für IP-Vernetzung mit Fax oder Modem Standardwert: EF
Prioritätsklasse für Netzwerksteuerung	Network Control, zum Beispiel SNMP-Traps Standardwert: CS7
Prioritätsklasse für Sprach-Payload	Voice-Payload für die IP-Telefonie (Voice over IP) Standardwert: EF

27.3.1.15 Grundeinstellungen > Datum und Uhrzeit > Datum und Uhrzeit

Parameterbeschreibung der Registerkarten:

- **Datum und Uhrzeit setzen**

Parameter	Beschreibung
Datum und Uhrzeit	
Tag	Auswahl des Tages.
Monat	Auswahl des Monats.
Jahr	Eingabe des Jahrs.
STD:MM:SS	Eingabe der Uhrzeit im 24-Stunden Format.

27.3.1.16 Grundeinstellungen > Datum und Uhrzeit > Zeitzonen-Einstellungen

Parameterbeschreibung der Registerkarten:

- **Zeitzonen-Einstellungen ändern**

Parameter	Beschreibung
Zeitzone	Lokale Zeitzone, in welcher sich das System befindet

27.3.1.17 Grundeinstellungen > Datum und Uhrzeit > SNTP-Einstellungen

Parameterbeschreibung der Registerkarten:

- **Einstellungen ändern**

Parameter	Beschreibung
SNTP-Client Eingabe der Zugangsdaten für einen externen Zeitserver (SNTP) zur netzweiten Synchronisation der Systemuhr.	
Administrativer Zustand des SNTP-Client	Verbindung des Kommunikationssystems zum SNTP-Server aktivieren oder. deaktivieren. Standardwert: Inaktiv
IP-Adresse/DNS-Name des externen Zeitservers	IP-Adresse oder DNS-Name des SNTP-Servers. Standardwert: 0.de.pool.ntp.org
Pollzeit für externen Zeitserver	Intervall für die Synchronisation von Datum und Uhrzeit mit dem SNTP-Server. Standardwert: 4 Std.

27.3.1.18 Grundeinstellungen > Port-Verwaltung

Die dargestellten Ports dienen zur Identifizierung der Netzwerkprotokolle und entsprechenden Netzwerkdienste. Einige der Ports, die das Kommunikationssystem selbst verwendet, können hier geändert werden. Dadurch kann z. B. in einem Netzwerk die Kommunikation auf das Kundennetz abgestimmt werden, wenn die Ports bereits anderweitig verwendet werden. Wenn an der Portverwaltung Änderungen vorgenommen werden, muss dies in der Regel an allen Komponenten (Telefone, Anlagen etc.) gleichzeitig geändert werden, damit die Funktionalität gewährleistet bleibt.

Parameterbeschreibung der Registerkarten:

- **Globale Port-Manager-Einstellungen ändern**

Parameter	Beschreibung
Protokoll-Name	Dienst.
Port-Nummer	Portnummer des Dienstes (konfigurierbar).
Port-Typ	Zur Information wird der Port-Typ angezeigt; Single: ein einzelner Port; Min: Untergrenze für ein Port-Bereich.
Dienste	
CSP	CSTA Service Provider, IP-Port für alle Applikationen, die sich mit dem CSP verbinden wollen. Standardwert: 8800
HFA	Steuerung von HFA-Clients (CorNet-TC Serverport). Standardwert: 4060

Parameter	Beschreibung
HFA_TLS	CorNet-TC über TLS. Standardwert: 4061
MEB_SIP	MediaExtensionBridge, Callsignalling für SIPQ Trunking. Standardwert: 15060
RTP_MIN	RTP/RTCP- und T.38-Ports (MediaBasePort). Standardwert: 29100
SIP	Rufsignalisierung für SIP-Endgeräte und SIP-basiertes Trunking. Standardwert: 5060
SIPS	Sichere Rufsignalisierung für SIPQ Trunking. Standardwert: 5061
SIP_TLS_SUB	Sichere Rufsignalisierung für SIP-Teilnehmer. Standardwert: 5062
VSL_MULTISITE	Multi-Site-Verbindungen. Standardwert: 8778

27.3.1.19 Grundeinstellungen > Gebühren > Gebühren Ausgabe

Parameterbeschreibung der Registerkarten:

- **Gebühren Ausgabe ändern**

Parameter	Beschreibung
Format des Gesprächsdatensatzes	
Komprimiertes Ausgabeformat	Standardwert: aktiviert
Letzten 4 Ziffern unterdrücken	Ersetzen der letzten 4 Ziffern des Feldes Rufnummer durch Fragezeichen zum Schutz der Privatsphäre. Standardwert: deaktiviert
Kommende Gespräche protokollieren	Standardwert: deaktiviert
Anrufdauerprotokollierung ein	Protokollierung der Gesprächsdauer in Stunden, Minuten und Sekunden. Standardwert: aktiviert
Anrufprotokoll ein	Bei kommenden Gesprächen wird unmittelbar nach Rufbeginn ein Verbindungsadensatz angelegt, z. B. für eine Anruferliste oder über eine PC-Auswertung des Datensatzes Zusatzinformationen zu den Anrufern zu übermitteln. Standardwert: deaktiviert
Ausgabe der MSN	Protokollierung der benutzten MSN (Nur IDSN) Standardwert: deaktiviert

Parameter	Beschreibung
Dezimalformat	(nicht in USA) Format der Gebührenanzeige, ist länderindividuell zu konfigurieren. In Deutschland wird immer das Dezimalformat verwendet. Gleichfalls bedeutet diese Dezimaldarstellung, dass der Multiplikator in Hundertstel angegeben wird. Der Multiplikator gibt an, mit welchem Betrag eine Tarifeinheit multipliziert wird, um den Währungsbetrag zu erhalten (z.B. 0,06 Euro statt 6 Cent). Standardwert: aktiviert
Beträge statt Einheiten ausgeben	Es werden Geldbeträge statt Tarifeinheiten ausgegeben (z. B. 4,50 EUR statt 75 Einheiten). Standardwert: aktiviert
Gehend ohne Verbindung	Protokollierung gehender Gespräche, welche nicht angenommen wurden. Standardwert: deaktiviert
Gebühren-Erfassung zentral	
Ausgabe: keine	Keine Übertragung von Verbindungsdaten Standardwert: HTTPS
Ausgabe: HTTPS	Übertragung von Verbindungsdaten an mitgelieferten Gebührenmanager oder andere Accounting-SW Standardwert: HTTPS
Ausgabe: LAN-TCP Client	Übertragung von Verbindungsdaten an externen Server via TCP/IP Standardwert: HTTPS
TCP-Client	Festlegen von IP-Adresse und Portnummer eines externen Gebührenservers. Bei anfallenden Gebühren initiiert das Kommunikationssystem eine TCP/IP-Verbindung zum externen Gebührenserver. Nach dem Verbindungsaufbau werden die Gebührendaten übertragen, die Verbindung bleibt permanent bestehen, weiter anfallende Gebühren werden versendet. Jeder Datensatz wird dabei einzeln verschickt.

27.3.1.20 Grundeinstellungen > Gebühren > Gebühren Faktoren

Parameterbeschreibung der Registerkarten:

- **Gebührenfaktoren ändern**

Parameter	Beschreibung
Gebührenfaktor pro Richtung	Die Gebühreninformation kann in Form von Tarifeinheiten (Zählimpulse) oder Währungseinheiten (Geldbeträge) angeboten werden. Beide Formen werden unterstützt, aber es werden nur Währungseinheiten am Display angezeigt. Bei Übermittlung der Information in Form von Gebühreneinheiten wird ein Umrechnungsfaktor benutzt. Diese Gebührenfaktoren werden pro Richtung eingestellt und gelten sowohl für Amtsgespräche als auch im Netzverbund, gehend und kommend.
Richtungen	Anzeige der im System vorhandenen Richtungen
Multiplikator	Dieser Multiplikator wird verwendet zur Umrechnung von Tarifeinheiten in Währungsbeträge. Wertebereich: 1 bis 65534, Standardwert: 6

Parameter	Beschreibung
Multipl. ISDN	Faktor zur zur Umrechnung empfangener bzw. zu versendender Währungsbeträge in Tarifeinheiten und umgekehrt. Nur für Richtungen mit Protokoll QSIG. Wertebereich: 1 bis 65535, Standardwert: 6
Währung	Kurzbezeichnung der Währung, z. B. EUR. Dies ist mit dem angeschlossenen Kommunikationssystem abzustimmen. Die Konfiguration des Währungsstrings ist unabhängig von dem Währungsstring für die Anzeige bei den Endgeräten. Hinweis: Der Parameter hat nur Bedeutung bei Richtungen mit Protokoll QSIG. Bei anderen Protokollen ist der Parameter wirkungslos und die vorgegebene Einstellung (Standardeinstellung) ist dann beizubehalten. Wertebereich: max. 3 Zeichen
Währungsbetrag	In der Spalte Währungsbetrag wird festgelegt, ob Währungsbeträge oder Tarifeinheiten auf der Richtung ausgetauscht werden. Bei aktivierter Option wird der Währungsbetrag versendet und empfangen (siehe Spalte Multipl. ISDN). Anderenfalls werden Tarifeinheiten versendet und empfangen. Dies ist mit dem angeschlossenen Kommunikationssystem abzustimmen. Wenn auf der Richtung Gebührenimpulse ausgetauscht werden, so sollte als Währung ein leerer String konfiguriert werden. Hinweis: Der Parameter hat nur Bedeutung bei Richtungen mit Protokoll QSIG. Bei anderen Protokollen ist der Parameter wirkungslos und die vorgegebene Einstellung (Standardeinstellung) ist dann beizubehalten.
Gebührenmode: keine Gebühren	Über die Richtung werden keine Gebühren empfangen, z.B. USA Amtsleitungen. Parameter ist nicht relevant bei Richtungen mit Protokoll QSIG.
Gebührenmode: während Verbindung	Gebühren werden nur während der Verbindung empfangen, nicht beim Verbindungsabbau.
Gebührenmode: am Ende der Verbindung	Gebühren werden nur bei Verbindungsende empfangen.
Gebührenmode: während/am Ende der Verbindung	Gebühren werden während einer Verbindung und bei Verbindungsabbau empfangen.
Währung	Währungskennzeichen für die Gebührenanzeige bei den Endgeräten.
Rechengenauigkeit	Ist so einzustellen, dass die Genauigkeit des Kommunikationssystems mindestens gleich groß ist als jene der vom Amt gesendeten Geldbeträge. Falls die maximal möglichen drei Nachkommastellen nicht ausreichen, wird automatisch gerundet. "Über Gebührenimpulse" ist zu wählen bei Richtungen mit Protokoll QSIG.

27.3.1.21 Grundeinstellungen > Gebühren > Gebühren Projekt Kennzahlen

Parameterbeschreibung der Registerkarten:

- **Projektkennzahlen ändern**

Parameter	Beschreibung
Prüfverfahren	
Prüfverfahren: Keine Prüfung	Keine Prüfung eingegebener Projekt-Kennzahlen unterzogen. Diese Option kann bei Richtungen mit Pflicht-Eingabe nicht verwendet werden.
Prüfverfahren: Listenprüfung	Eingegebene PKZ werden an Hand der PKZ-Listen auf Gültigkeit geprüft.

Parameter	Beschreibung
Prüfverfahren: Prüfung der Stellenanzahl	Eingegebene PKZ werden auf ihre Stellenanzahl geprüft.
Anzahl der zu prüfenden Stellen	Gültige Stellenanzahl für PKZ. Wertebereich: 1 - 11, Standardwert: 5
PKZ-Listen	
Liste	Für Listenprüfung können maximal 1000 PKZ eingegeben werden.
Projektkennzahl	Wertebereich: max. 11 Ziffern

27.3.1.22 Grundeinstellungen > Wiedergabegerät für Sprachnachrichten/Ansagen

Parameterbeschreibung der Registerkarten:

- **Wiedergabegerät für Sprachnachrichten/Ansagen ändern**

Parameter	Beschreibung
Voicemail	
Präfix	Rufnummer der Sprachbox.
Wiedergabegerät für Ansagen	
Rufnummer	Rufnummer des Wiedergabegeräts (Announcement Player).

27.3.1.23 Grundeinstellungen > Telefonparameter-Bereitstellung

Parameterbeschreibung der Registerkarten:

- **Telefonparameter-Bereitstellung ändern**

Parameter	Beschreibung
Telefonparameter-Bereitstellung Voraussetzung für die Wirksamkeit dieser Parameter ist, dass die Systemtelefone den DLI des Systems nutzen und dieser die Systemtelefone mit den nötigen Paramentern versorgen kann. Die Parameter der Systemtelefone werden aktualisiert, sobald sich ein Systemtelefon neu mit dem System verbindet oder neu gestartet wird oder das System neu gestartet wird. Die individuellen Parameter können direkt am Systemtelefon oder mit dem WBM des Systemtelefons konfiguriert werden. Die Einstellungen für den PC Ethernet Port und für die Codec-Priorisierung werden vom DLI nicht überschrieben, wenn sie direkt am Systemtelefon oder mit dem WBM des Systemtelefons konfiguriert wurden.	
PC-Port-Modus	Ist dieses Flag aktiviert, wird der PC Ethernet Port aller aktiven Systemtelefone eingeschaltet. Standard: Deaktiviert
Codec setting is "low bandwidth preferred"	Ist dieses Flag aktiviert, gilt für alle Systemtelefone folgende Codec-Priorisierung: G.729 - G.711 - G.722 Ist dieses Flag deaktiviert, gilt folgende Codec-Priorisierung: G.722 - G.711 - G.729 Standard: Deaktiviert
Bilder für Anrufer anzeigen	Ist dieses Flag aktiviert, wird an Systemtelefonen mit großem Farbdisplay bei einem ankommenden Ruf das Bild des Anrufers angezeigt, sofern es über UC Smart oder UC Suite in das System geladen wurde. Standard: Deaktiviert
Modus und Codec-Einstellungen für alle Telefone zurücksetzen	Ist dieses Flag aktiviert, werden an allen Systemtelefonen der PC Ethernet Port deaktiviert und die Codec-Einstellungen auf die Standardwerte zurückgesetzt. Standard: Deaktiviert

27.3.1.24 Grundeinstellungen > Power Management

Parameterbeschreibung der Registerkarten:

- **Power Management ein-/ausschalten**

Parameter	Beschreibung
Power Management Das Power-Management kann nur aktiviert werden, wenn sich die LAN-Schnittstellen des Systems im Ethernet-Link-Modus **Auto** befinden. Im Energiesparzustand wechseln die LAN-Schnittstellen des Systems automatisch in den 100Mbit/s-Vollduplex-Modus. Die LAN-Schnittstellen der angeschlossenen Infrastruktur sollten sich ebenfalls im Autosense-Modus befinden.	
Power Management ein-/ausschalten	Schaltet das System in den Energiesparzustand.
Beginn des LowPowerModes	Startzeitpunkt des Energiesparzustand.
Ende des LowPowerModes	Endzeitpunkt des Energiesparzustand.
IP Bandbreite wird auf 100MBit/s FDX reduziert	Anzeige der Datenrate im Energiesparzustand.

27.3.2 Sicherheit

Unter **Sicherheit** sind die sicherheitsrelevanten Einstellungen zusammengefasst. Dazu gehören Einstellungen für Firewall, Filter, VPN und SSL.

27.3.2.1 Sicherheit > Application Firewall

Parameterbeschreibung der Registerkarten:

- **Services anzeigen**
- **Service hinzufügen**
- **Alle Services löschen**

Parameter	Beschreibung
Application Firewall	Die Application Firewall dient der Beschränkung des Zugriffs auf bestimmten Diensten (Services), wie z. B. FTP oder LDAP. Sie ist im Auslieferungszustand ausgeschaltet und lässt sich nach Definition entsprechender Regeln aktivieren. Folgende Dienste können durch die Application Firewall auf bestimmte IP-Adressen oder IP-Adressbereiche beschränkt oder gesperrt werden: **Dienst / Ports** HTTPS / 443 Postgres / 5432 OpenScape Business Status / 8808 CSTA / 7001 (FP), 7004 (FP), 8800 (CSP) LDAP / 389 Manager E / 7000 ssh (im Default gesperrt) / 22 FTP / 21, 40000 - 40040 Nur die gelisteten Dienste können über ein Auswahlmenü im Expertenmodus gesperrt werden. Telefonleistungsmerkmale wie SIP, HFA usw. können nicht über die Application Firewall gesperrt werden. Ein Dienst kann mehrmals ausgewählt werden, jeweils mit unterschiedlichen IP-Restriktionen.
Regelname	Vergebener Name für die Regel
Regel aktiviert	
Untergrenze des Quell-IP-Adressbereichs	
Obergrenze des Quell-IP-Adressbereichs	

27.3.2.2 Sicherheit > Deployment- und Licensing-Client (DLSC)

Um DLS-Funktionen nutzen zu können, muss das Kommunikationssystem dem externen DLS den Zugriff auf die Konfigurationsdaten gewähren. Das Kommunikationssystem wird dann als Deployment und Licensing Client betrieben. Der externe DLS-Server wird unter > Mainboard > DHCP-Modus > DHCPServer > Globale Einstellungen eingerichtet.

Parameterbeschreibung der Registerkarten:

- **DLSC-Grundeinstellung**
- **DLSC Kontaktieren**
- **DLSC Bootstrapping zurücksetzen**

Parameter	Beschreibung
Status	
Sichere Kommunikation mit DLS Client	Anzeige, ob (und wieviel) eine sichere Kommunikation mit dem DLS-Client aktiviert bzw. deaktiviert (0) ist.
DLS-Client	
Zeitinterval für ContactMe-Antwort	Standardwert: 0
PIN für DLS-Bootstrapping erforderlich	erhöhte Sicherheitsstufe durch PIN-Eingabe auf beiden Seiten
Bootstrap PIN	Wertebereich: min. 8 bis max. 32 Zeichen
DLS-Server	
IP-Adresse des DLS-Servers	Eintrag der IP-Adresse des externen DLS-Servers.
Port des DLS-Servers	Port-Eingabe des externen DLS-Servers Standardwert: 18443
Port für sichere Verbindung zum DLS-Server	Anzeige der Portnummer für eine sichere Verbindung

27.3.2.3 Sicherheit > Deployment- und Licensing-Client (DLSC) > DLSC-Client-Zertifikat

Parameterbeschreibung der Registerkarten:

- **Zertifikatsinformationen**

Parameter	Beschreibung
Zertifikatstyp	Dient dem sicheren Erstkontakt zwischen dem Kommunikationssystem und dem DLS
Seriennummer des Zertifikats	Anzeige der festgelegten Seriennummer.
Seriennummer des Zertifikats (hex)	

Parameter	Beschreibung
Signatur-Algorithmus-Typ	Anzeige des verwendenden Signaturalgorithmus Wertebereich: md5RSA, sha1RSA, sha256RSA, sha512RSA
Beginn der Zertifikatsgültigkeit (GMT)	Anzeige des Beginns der Zertifikatsgültigkeit. Die Zeitangabe wird als Greenwich Mean Time (GMT) interpretiert.
Ende der Zertifikatsgültigkeit (GMT)	Anzeige des Endes der Zertifikatsgültigkeit. Die Zeitangabe wird als Greenwich Mean Time (GMT) interpretiert.
CRL-Verteilerpunkt	Anzeige der optionalen URL, von der aus Zertifikatssperrlisten (CRL) verteilt werden
Ausgestellt durch CA	
Land (C)	
Organisation (O)	
Organisationseinheit (OU)	
Allgemeiner Name (CN)	
Antragsteller	Anzeige der Daten zum Zertifikatsantragsteller gemäß den Konventionen des Standards X.509 ein (z. B. im Feld Land (C) DE für Deutschland)
Land (C)	
Organisation (O)	
Organisationseinheit (OU)	
Allgemeiner Name (CN)	
Alternativer Antragsteller	Diese optionale Angabe unterscheidet zwischen Format des DN-Namens (Angaben wie unter Antragsteller) und Anderes Format (z. B. Eintrag einer IP-Adresse). Die Eingabemaske ist von der Auswahl des Formats abhängig
Daten des öffentl. Schlüssels	
Länge des öffentl. Schlüssels	
Öffentlicher Schlüssel	Verschlüsselung mit Hilfe öffentlicher Schlüssel, die von einer dritten Partei nach dem X.509-Standard bestätigt werden. Die hohe Sicherheit wird dadurch garantiert, dass der Schlüssel zur Dechiffrierung nochmals individuell festgelegt werden muss und nur beim Anwender gespeichert ist.
Fingerabdruck	Der verwendete öffentliche Schlüssel sowie der Fingerabdruck werden hexadezimal dargestellt.

27.3.2.4 Sicherheit > Deployment- und Licensing-Client (DLSC) > DLSC-CA-Zertifikat

Parameterbeschreibung der Registerkarten:

- **Zertifikatsinformationen**

Parameter	Beschreibung
Zertifikatstyp	Dient dem sicheren Erstkontakt zwischen dem Kommunikationssystem und dem DLS.
Seriennummer des Zertifikats	Anzeige der festgelegten Seriennummer.
Seriennummer des Zertifikats (hex)	
Signatur-Algorithmus-Typ	Anzeige des verwendenden Signaturalgorithmus. Wertebereich: md5RSA, sha1RSA, sha256RSA, sha512RSA
Beginn der Zertifikatsgültigkeit (GMT)	Anzeige des Beginns der Zertifikatsgültigkeit. Die Zeitangabe wird als Greenwich Mean Time (GMT) interpretiert.
Ende der Zertifikatsgültigkeit (GMT)	Anzeige des Endes der Zertifikatsgültigkeit. Die Zeitangabe wird als Greenwich Mean Time (GMT) interpretiert.
CRL-Verteilerpunkt	Anzeige der optionalen URL, von der aus Zertifikatssperrlisten (CRL) verteilt werden.
Ausgestellt durch CA	
Land (C)	
Organisation (O)	
Organisationseinheit (OU)	
Allgemeiner Name (CN)	
Antragsteller	Anzeige der Daten zum Zertifikatsantragsteller gemäß den Konventionen des Standards X.509 ein (z. B. im Feld Land (C) DE für Deutschland).
Land (C)	
Organisation (O)	
Organisationseinheit (OU)	
Allgemeiner Name (CN)	
Alternativer Antragsteller	Diese optionale Angabe unterscheidet zwischen Format des DN-Namens (Angaben wie unter Antragsteller) und Anderes Format (z. B. Eintrag einer IP-Adresse). Die Eingabemaske ist von der Auswahl des Formats abhängig.
Daten des öffentl. Schlüssels	
Länge des öffentl. Schlüssels	
Öffentlicher Schlüssel	Verschlüsselung mit Hilfe öffentlicher Schlüssel, die von einer dritten Partei nach dem X.509-Standard bestätigt werden. Die hohe Sicherheit wird dadurch garantiert, dass der Schlüssel zur Dechiffrierung nochmals individuell festgelegt werden muss und nur beim Anwender gespeichert ist.
Fingerabdruck	Der verwendete öffentliche Schlüssel sowie der Fingerabdruck werden hexadezimal dargestellt.
Zertifikatstyp	Dient dem sicheren Erstkontakt zwischen dem Kommunikationssystem und dem DLS.

27.3.2.5 Sicherheit > Signaling- und Payload-Encryption

Parameterbeschreibung der Registerkarten:

- **SPE Sicherheitseinstellungen ändern**

Parameter	Beschreibung
Minimale Länge des RSA-Schlüssels	Minimale Länge des RSA-Schlüssels in den Zertifikaten. Je größer dieser Wert ist, desto sicherer ist der Schlüssel Wertebereich: 512, 1024, 2048
Zertifikatüberprüfung mit CRL-Überprüfung	Mit Hilfe einer Zertifikatssperrliste (CRL: Certificate Revocation List) kann festgestellt werden, ob ein Zertifikat gesperrt/widerrufen wurde und warum. Erklärt eine Zertifizierungsstelle (CA: Certificate Authority) ein Zertifikat für ungültig, trägt es dessen Seriennummer in seine Liste ein. Während der Zertifikatsüberprüfung kann diese Liste über das Internet bei der Zertifizierungsstelle abgefragt werden Standard deaktiviert
Maximales Intervall für Schlüssel-Neuverhandlung (Stunden)	Dieses Intervall legt fest, wie lange ein bestimmter Schlüssel für die Verschlüsselung der Signalisierungs- und Nutzdaten verwendet werden soll. Nach Ablauf dieser Zeitdauer wird ein neuer Schlüssel festgelegt Wertebereich: 6 bis 48
Subjectname überprüfen	Durch Überprüfen des Subjectname im Zertifikat eines Gateways kann dessen Identität überprüft werden. Der Subjectname enthält die IP-Adresse oder den DNS-Namen (DNS: Domain Name System) des jeweiligen Gateways
Salt Key Verfahren verwenden	Mit diesem Verfahren können Passwörter stark verschlüsselt werden. Deren Entschlüsselung kann durch dieses Verfahren wesentlich erschwert oder sogar weitestgehend unmöglich gemacht werden. So ist zum Beispiel nach einer Verschlüsselung nicht mehr erkennbar, ob zwei Benutzer das gleiche Passwort verwenden
SRTP Authentifizierung notwendig	Durch die SRTP-Authentifizierung kann überprüft werden: - ob die Nutzdaten-Message eines VoIP-Clients unverfälscht ist - ob eine Nutzdaten-Message bereits einmal empfangen wurde. Dadurch werden Fälschungen der Nutzdaten und Replay-Attacken vermieden
SRTCP Verschlüsselung notwendig	Durch die SRTCP-Authentifizierung kann überprüft werden: - ob die Nutzdaten-Message eines VoIP-Clients unverfälscht ist - ob eine Nutzdaten-Message bereits einmal empfangen wurde. Dadurch werden Fälschungen der Nutzdaten und Replay-Attacken vermieden
Länge des SRTP/SRTPC Authentifizierungs-Tag	Das Authentifizierungs-Tag wird an ein Datenpaket angehängt, um dessen Unverfälschtheit sicherzustellen. Die Länge des Tags ist nicht änderbar

27.3.2.6 Sicherheit > Signaling- und Payload-Encryption > SPE Zertifikat

Parameterbeschreibung der Registerkarte:

- **SPE Zertifikat und privaten Schlüssel importieren (PKCS#12)**

Parameter	Beschreibung
Entschlüsselungskennwort	Eingabe des Kennworts, das bei der Erstellung der PKCS#12-Datei verwendet wurde.
Datei mit Zertifikat und privatem Schlüssel (PEM- oder PKCS#12-Format)	Auswahl der Datei, die die zu importierenden Zertifikats-Daten enthält.

27.3.2.7 Sicherheit > Signaling- und Payload-Encryption > SPE CA Zertifikate

Es können z. B. von einer Kunden PKI-Zertifizierungsstelle (RA/CA) bis zu 16 vertrauenswürdige CA-Zertifikate einzeln importiert werden.

Parameterbeschreibung der Registerkarte:

- **Vertrauenswürdiges CA-Zertifikat (X.509 Datei) für SPE importieren**

Parameter	Beschreibung
Datei mit Zertifikat (PEM oder Binär-Format)	Auswahl der zu importierenden PEM- oder Binär-Datei.
CRL Distribution Point (CDP) Protokoll	Protokollauswahl für die CRL-Listen (Zertifikatswiderrufslisten) Wertebereich: LDAP oder HTTP
CDP (ohne z.B. ldap://)	Ein CDP ist eine optionale Zertifikatserweiterung. Ein empfangenes Zertifikat wird nur gegen die CRLs geprüft, für die der CDP konfiguriert wurde.

27.3.2.8 Sicherheit > VPN

Parameterbeschreibung der Registerkarten:

- **Allgemeine Informationen anzeigen**
- **Aktivieren der konfigurierten VPN-Tabellen**
- **Ipsec ein-/ausschalten**

Parameter	Beschreibung
Verschlüsselungsalgorithmen	Verwendete Verschlüsselungsalgorithmen Wertebereich: AES, 3DES
Hash-Algorithmen	Standardisierte kryptologische Hashfunktion zur Berechnung eines eindeutligen Prüfwerts (digitale Signatur) Wertebereich: MD5, SHA1, SHA2
Public-Key-Algorithmen	asymetrisches Verschlüsselungsverfahren Wertebereich: RSA
Diffie-Hellman-Gruppen	Verfahren zum Austausch von Schlüssel Wertebereich: DH-Gruppe 2, DH-Gruppe 5
Schaltflächen	
Sofort aktivieren	Die VPN-Tabellen können aktiviert werden. Warnhinweise beachten!
Ipsec aktivieren / deaktivieren	IPsec kann aktiviert oder deaktiviert werden. Warnhinweise beachten!

27.3.2.9 Sicherheit > VPN > Lightweight CA

Parameterbeschreibung der Registerkarten:

- **CA-Zertifikat generieren**

Parameter	Beschreibung
Name des Zertifikats	Frei einzugebener Name des zu generierenden Zertifikates
Seriennummer des Zertifikats	Eingabe einer von Ihnen festgelegten Seriennummer. Die Nummer muss eine positive ganze Zahl sein.
Signatur-Algorithmus-Typ	Auswahl des für dieses Zertifikat zu verwendenden Signaturalgorithmus Wertebereich: md5RSA, sha1RSA, sha25RSA, sha512RSA
Länge des öffentlichen Schlüssels	Auswahl einer für dieses Zertifikat verwendeten Schlüssellänge Wertebereich: 1024, 1536, 2048
Beginn der Zertifikatsgültigkeit (GMT) Zeiteingabe, ab wann das Zertifikat gültig sein soll. Die Zeitangabe wird als Greenwich Mean Time (GMT) interpretiert.	
Ende der Zertifikatsgültigkeit (GMT) Zeiteingabe, bis wann das Zertifikat gültig sein soll. Die Zeitangabe wird als Greenwich Mean Time (GMT) interpretiert.	
Antragsteller Eingabe der Daten zum Zertifikatsantragsteller gemäß den Konventionen des Standards X.509 ein (z. B. im Feld Land (C) DE für Deutschland).	
Alternativer Antragsteller Diese optionale Angabe unterscheidet zwischen Format des DN-Namens (Angaben wie unter Antragsteller) und einem anderen Format (z. B. Eintrag einer IP-Adresse). Die Eingabemaske ist von der Auswahl des Formats abhängig.	
Format des DN-Namens	
Anderes Format	
Erweiterung Alternativer Antragstellername	Wertebereich: DNS-Name, IP-Adresse, E-Mail-Adresse, Uniform resource Indicator, Andere
Alternativer Antragsteller	
CRL-Verteilungspunkt-Typ	Wertebereich: DNS-Name, IP-Adresse, E-Mail-Adresse, Uniform resource Indicator, Andere
CRL-Verteilungspunkt	Angabe einer URL, von der aus Zertifikatssperrlisten (CRL) verteilt werden.
Zertifikat erzeugen	

27.3.2.10 Sicherheit > VPN > Zertifikatsverwaltung

Parameterbeschreibung der Registerkarten:

- **Zertifikat aus Datei anzeigen**

Parameter	Beschreibung
PKCS#12-Format	Falls das Zertifikat in einer PKCS#12-Datei gespeichert ist, müssen Sie dieses Feld aktivieren.
Entschlüsselungskennwort	Wenn das Feld PKCS#12-Format aktiviert wurde, müssen Sie in diesem Feld das gleiche Kennwort angeben, das bei der Dateierstellung verwendet wurde.
Datei mit dem Zertifikat	Tragen Sie in diesem Feld den Pfad und den Dateinamen des Zertifikats ein. Klicken Sie auf Durchsuchen, falls Sie den Speicherort nicht genau kennen. Ein Suchdialog wird angezeigt.

27.3.2.11 Sicherheit > VPN > Zertifikatsverwaltung > Trusted CA Zertifikate > Aktive Zertifikate

Parameterbeschreibung der Registerkarte:

- **Trusted CA-Zertifikat importieren (X509)**

Parameter	Beschreibung
Zertifikatstyp	Dient dem sicheren Erstkontakt zwischen dem Kommunikationssystem und dem DLS
Seriennummer des Zertifikats	Anzeige der festgelegten Seriennummer.
Seriennummer des Zertifikats (hex)	
Signatur-Algorithmus-Typ	Anzeige des verwendenden Signaturalgorithmus Wertebereich: md5RSA, sha1RSA, sha256RSA, sha512RSA
Beginn der Zertifikatsgültigkeit (GMT)	Anzeige des Beginns der Zertifikatsgültigkeit. Die Zeitangabe wird als Greenwich Mean Time (GMT) interpretiert.
Ende der Zertifikatsgültigkeit (GMT)	Anzeige des Endes der Zertifikatsgültigkeit. Die Zeitangabe wird als Greenwich Mean Time (GMT) interpretiert.
CRL-Verteilerpunkt	Anzeige der optionalen URL, von der aus Zertifikatssperrlisten (CRL) verteilt werden
Ausgestellt durch CA	
Land (C)	
Organisation (O)	
Organisationseinheit (OU)	
Allgemeiner Name (CN)	
Antragsteller	Anzeige der Daten zum Zertifikatsantragsteller gemäß den Konventionen des Standards X.509 ein (z. B. im Feld Land (C) DE für Deutschland)
Land (C)	
Organisation (O)	
Organisationseinheit (OU)	

Parameter	Beschreibung
Allgemeiner Name (CN)	
Alternativer Antragsteller	Diese optionale Angabe unterscheidet zwischen Format des DN-Namens (Angaben wie unter Antragsteller) und Anderes Format (z. B. Eintrag einer IP-Adresse). Die Eingabemaske ist von der Auswahl des Formats abhängig
Daten des öffentl. Schlüssels	
Länge des öffentl. Schlüssels	
Öffentlicher Schlüssel	Verschlüsselung mit Hilfe öffentlicher Schlüssel, die von einer dritten Partei nach dem X.509-Standard bestätigt werden. Die hohe Sicherheit wird dadurch garantiert, dass der Schlüssel zur Dechiffrierung nochmals individuell festgelegt werden muss und nur beim Anwender gespeichert ist.
Fingerabdruck	Der verwendete öffentliche Schlüssel sowie der Fingerabdruck werden hexadezimal dargestellt.

27.3.2.12 Sicherheit > VPN > Zertifikatsverwaltung > Trusted CA Zertifikate > Konfigurierte Zertifikate

Parameterbeschreibung der Registerkarte:

- **Trusted CA-Zertifikat importieren (X509)**

Parameter	Beschreibung
Name des Zertifikats	Eingabe des Namens, den das Zertifikat haben soll.
Datei mit dem Zertifikat	Pfad und Dateinamen des Zertifikats. Beim Anklicken von Durchsuchen wird ein Suchdialog angezeigt, um den Speicherort der Datei zu finden.

27.3.2.13 Sicherheit > VPN > Peer-Zertifikate

Parameterbeschreibung der Registerkarten:

- **Zertifikatsanforderung (CSR) generieren**
- **Peer-Zertifikat importieren (PKCS#12)**

Parameter	Beschreibung
Name der Zertifikatsanforderung	Ein CA-signiertes Peer-Zertifikat (das auf einem CA-Zertifikat basiert) kann erzeugt werden. Voraussetzung ist, dass mindestens ein CA-Zertifikat generiert wurde. Das erzeugte Zertifikat wird in einer PKCS#12-Datei gespeichert. PKCS#12- Dateien (PKCS#12 Personal Information Exchange Syntax Standard) speichern Zertifikate mit dem privaten Schlüssel. Eine PKCS#12-Datei enthält also die entscheidenden Daten für persönliche Ver- und Entschlüsselung.
Signatur-Algorithmus-Typ	Wählen Sie den für dieses Zertifikat zu verwendenden Signaturalgorithmus aus. Wertebereich: md5RSA, sha1RSA, sha25RSA, sha512RSA
Länge des öffentlichen Schlüssels	Wertebereich: 1024, 1536, 2048
Antragsteller	Angabe der Daten zum Zertifikatsantragsteller gemäß den Konventionen des Standards X.509 ein (z. B. im Feld Land (C) DE für Deutschland).
Land (C)	
Organisation (O)	
Organisationseinheit (OU)	
Allgemeiner Name (CN)	
Alternativer Antragsteller	Diese optionale Angabe unterscheidet zwischen Format des DN-Namens (Angaben wie unter Antragsteller) und Anderes Format (z. B. Eintrag einer IP-Adresse). Die Eingabemaske ist von der Auswahl des Formats abhängig.
Format des DN-Namens	
Land (C)	
Organisation (O)	
Organisationseinheit (OU)	
Allgemeiner Name (CN)	
Anderes Format	
Erweiterung Alternativer Antragstellername	Wertebereich: DNS-Name, IP-Adresse, E-Mail-Adresse, Uniform resource Indicator, Andere
Alternativer Antragstellername	Diese optionale Angabe unterscheidet zwischen Format des DN-Namens (Angaben wie unter Antragsteller) und Anderes Format (z. B. Eintrag einer IP-Adresse). Die Eingabemaske ist von der Auswahl des Formats abhängig.
Peer-Zertifikat importieren [PKCS#12]	
Name des Zertifikats	
Entschlüsselungskennwort	Kennwort zur Entschlüsselung des Peer-Zertifikats Wertebereich: min. 7 und max. 32 Zeichen

Parameter	Beschreibung
Datei mit dem Zertifikat	Klicken Sie auf Durchsuchen. Ein Suchdialog wird dann angezeigt.
Fingerabdruck des Zertifikats anzeigen	
Zertifikat aus Datei importieren	

27.3.2.14 Sicherheit > VPN > Dienste > Aktive Dienste

Parameterbeschreibung der Registerkarte:

- **Ipsec-Dienste anzeigen**

Parameter	Beschreibung
Name des Dienstes	Dieses Feld enthält die Namen der konfigurierten Dienste.
Status im IP-Stack	
Quell-Port	Anzeige der Quell-Port-Nummer. Wird als Port die "0" angezeigt, so entspricht das einem beliebigen bzw. unbekannten Port.
Ziel-Port	Anzeige der Ziel-Port-Nummer. Wird als Port die "0" angezeigt, so entspricht das einem beliebigen bzw. unbekannten Port.
IP-Protokoll	Anzeige des für die Übertragung verwendeten IP-Protokolls.
Zugehörige 'pass'-Regel	Anzeige der zugehörigen "Pass"-Regel. Die Zuordnung von Regeln und Diensten erfolgt bei den Regeln.
Zugehörige 'deny'-Regel	Anzeige der zugehörigen "Deny"-Regel. Die Zuordnung von Regeln und Diensten erfolgt bei den Regeln.

27.3.2.15 Sicherheit > VPN > Dienste > Konfigurierte Dienste

Parameterbeschreibung der Registerkarten:

- **Ipsec-Dienste anzeigen**
- **Ipsec-Dienste hinzufügen**
- **Ipsec-Dienste ändern**
- **Ipsec-Dienste umbenennen**
- **Ipsec-Dienste löschen**

Parameter	Beschreibung
Name des Dienstes	Eingabefeld für den Namen des zu konfigurierten Dienstes. Geben Sie eine Zeichenkette in dieses Feld ein.
Quell-Port	Nummer des Ports, der für die Übertragung der Daten auf der Sendeseite verwendet werden soll. Wird als Port die "0" eingetragen, so entspricht das einem beliebigen bzw. unbekannten Port.
Ziel-Port	Nummer des Ports, der für die Übertragung der Daten auf der Empfängerseite verwendet werden soll. Wird als Port die "0" eingetragen, so entspricht das einem beliebigen bzw. unbekannten Port.
IP-Protokoll	Für die Übertragung zu verwendende IP-Protokoll Wertebereich: ICMP, TCP, UDP
Name des Dienstes	Eingabefeld für den Namen des zu konfigurierten Dienstes.
Quell-Port	Nummer des Ports, der für die Übertragung der Daten auf der Sendeseite verwendet werden soll. Wird als Port die "0" eingetragen, so entspricht das einem beliebigen bzw. unbekannten Port.
Ziel-Port	Nummer des Ports, der für die Übertragung der Daten auf der Empfängerseite verwendet werden soll. Wird als Port die "0" eingetragen, so entspricht das einem beliebigen bzw. unbekannten Port.
IP-Protokoll	Wählen Sie die für die Übertragung verwendete IP-Protokoll aus Wertebereich: ICMP, TCP, UDP
Name des Dienstes	Eingabefeld für den Namen des zu konfigurierten Dienstes.
	Löschen ist nur möglich wenn dem Dienst keine Regel zugeordnet ist.

27.3.2.16 Sicherheit > VPN > Tunnel > Aktive Tunnel

Parameterbeschreibung der Registerkarten:

- **Allgemeine Tunneldaten anzeigen**
- **Regeln für alle Tunnel anzeigen**

Parameter	Beschreibung
Name des Tunnels	Dieses Feld enthält den Namen des konfigurierten Tunnels.
Status im IP-Stack	Statusanzeige im IP-Stack. Wertebereich: aktiv / nicht aktiv
Endpunkttyp des lokalen Tunnel	Anzeige der Endpunktadresse auf der Tunnel-Sendeseite (möglich sind die Angabe eines Host- oder DNS-Namens).
Endpunktadresse des lokalen Tunnel	Anzeige der Endpunktadresse im lokalen Tunnel.
Endpunkttyp des Remote Tunnel	Anzeige des Endpunkttyps des Remote-Tunnels.

Parameter	Beschreibung
Endpunktadresse des Remote Tunnel	Anzeige der Empfängeradresse des Remote-Tunnels. Wird die Adresse 0.0.0.0 angezeigt, so bedeutet dies, dass der Tunnelendpunkt unbekannt ist. In diesem Fall muss der Tunnelaufbau immer von der Gegenstelle erfolgen (z.B. Teleworker).
Vorgeschlagene Lebensdauer der Session-Keys	Anzeige der akzeptierten Gültigkeitsdauer für die Sitzungsschlüssel (Session Keys), die verwendet werden. Nach Ablauf dieser Zeit werden keine Daten mehr innerhalb dieser Sitzung ausgetauscht. Als Ersatz für ungültig gewordene Sitzungsschlüssel werden automatisch neue Sitzungsschlüssel ausgehandelt.
Vorgeschlagene Lebensdauer der Schlüsseltausch-Session	Anzeige der akzeptierten Gültigkeitsdauer für die Schlüsseltausch-Session. Nach Ablauf der Schlüsseltausch-Session werden automatisch neue Schlüssel für die Schlüsseltausch-Session durch IKE (Verschlüsselungsprotokoll) ausgehandelt.
Zugehörige Regeln: Zugehörige Senderegel	Einrichtung der Senderegel unter VPN>Regeln
Zugehörige Regeln: Zugehörige Empfangsregel	Einrichtung der Empfangsregel unter VPN>Regeln
Tunneldaten	
Name des Tunnels	Dieses Feld enthält den Namen des konfigurierten Tunnels.
Status im IP-Stack	Statusanzeige im IP-Stack. Wertebereich: aktiv / nicht aktiv
Endpunkttyp des lokalen Tunnel	Anzeige der Endpunktadresse auf der Tunnel-Sendeseite (möglich sind die Angabe eines Host- oder DNS-Namens).
Endpunktadresse des lokalen Tunnel	Anzeige der Endpunktadresse im lokalen Tunnel.
Endpunkttyp des Remote Tunnel	Anzeige des Endpunkttyps des Remote-Tunnels.
Endpunktadresse des Remote Tunnel	Anzeige der Empfängeradresse des Remote-Tunnels. Wird die Adresse 0.0.0.0 angezeigt, so bedeutet dies, dass der Tunnelendpunkt unbekannt ist. In diesem Fall muss der Tunnelaufbau immer von der Gegenstelle erfolgen (z. B. Teleworker).
Regeldaten	
Richtung	
Priorität	Anzeige der Priorität für die Abarbeitungsfolge. Die höchste Priorität wird mit 1 angegeben. Für jede Regel einer Richtung ist eine eigene Priorität zu vergeben. Eine Regel und die dazugehörige Regel der Gegenrichtung müssen stets die gleiche Priorität haben. Die Regel für die Gegenrichtung können Sie nur über den entsprechenden Menüpunkt einrichten.
Aktion für die Regel	Anzeige der IP-Pakete, wie diese mit der Regel zu behandeln sind: pass bedeutet, IP-Pakete werden weitergeleitet, deny bedeutet, es werden keine IP-Pakete weitergeleitet.
Verschlüsselung erforderlich	Anzeige einer Verschlüsselung für diese Regel. Das Verschlüsselungsverfahren wird über den zugeordneten Tunnel definiert.
Regel-Status	
Status im IP-Stack	Statusanzeige im IP-Stack. Wertebereich: aktiv / nicht aktiv

Parameter	Beschreibung
Quelladresse Anzeige der Quell- und Zieladresse in dem Format, das zum gewählten Typ passt. Die Anzeige ist vom gewählten Adresstyp abhängig. Wenn jede beliebige IP-Adresse genutzt werden soll, wird 0.0.0.0 angezeigt. Wird als Zieladresse 0.0.0.0 angegeben, um Pakete in einen Tunnel zu schicken, so muss an der Schnittstelle zum Zielnetzwerk NAT deaktiviert werden. Alternativ ist auch eine IP-Angabe zwischen 0.0.0.1 und 255.255.255.254 möglich, um Pakete in einen Tunnel zu schicken.	
Typ	Anzeige des Typs für die Quelladresse und die Zieladresse (möglich sind: Host, Subnetz, IP Adressbereich und DNS-Name).
Adresse (unterste des Bereichs)	
Subnetzmaske / oberste Adr. des Bereichs	
Zieladresse	
Typ	Anzeige des Typs für die Quelladresse und die Zieladresse (möglich sind: Host, Subnetz, IP Adressbereich und DNS-Name).
Adresse (unterste des Bereichs)	Anzeige der Quell- und Zieladresse in dem Format, das zum gewählten Typ passt. Die Eingabemaske ist vom gewählten Adresstyp abhängig. Wenn jede beliebige IP-Adresse genutzt werden soll, wird 0.0.0.0 angezeigt. Wird als Zieladresse 0.0.0.0 angegeben, um Pakete in einen Tunnel zu schicken, so muss an der Schnittstelle zum Zielnetzwerk NAT deaktiviert werden. Alternativ ist auch eine IP-Angabe zwischen 0.0.0.1 und 255.255.255.254 möglich, um Pakete in einen Tunnel zu schicken.
Subnetzmaske / oberste Adr. des Bereichs	
Dienstdaten Anzeige des Dienstes, welche auf die Verschlüsselung beschränkt wurde. Soll die Verschlüsselung nicht auf einen Dienst beschränkt sein, wählen Sie "Beliebiger Dienst" aus.	
Name des Dienstes	
Quell-Port	Anzeige des Tunnels in Empfangsrichtung, für den diese Regel gilt. Aus diesem Tunnel werden die IP-Pakete, die vom Netz empfangen werden, abgeholt. Wählen Sie Keine Tunnelzuordnung, falls in Empfangsrichtung kein Tunnel zugeordnet werden soll.
Ziel-Port	Anzeige des Tunnels in Senderichtung, für den diese Regel gilt. In diesen Tunnel werden die IP-Pakete, die zum Netz gesendet werden müssen, hineingeschickt. Wählen Sie Keine Tunnelzuordnung, falls in Senderichtung kein Tunnel zugeordnet werden soll.
IP-Protokoll	

27.3.2.17 Sicherheit > VPN > Tunnel > Konfigurierte Tunnel

Parameterbeschreibung der Registerkarten:

- **Allgemeine Tunneldaten anzeigen**
- **Regeln für alle Tunnel anzeigen**
- **Tunnel hinzufügen / Tunneldaten ändern**
- **Schlüsselaustauschdaten**

Parameter	Beschreibung
	Ein Tunnel bezeichnet einen Transport von verschlüsselten Datenpaketen zu einem fest definierten Endpunkt. Aktive Tunnel sind konfigurierte Tunnel nach einer Aktivierung der Konfiguration. Insgesamt lassen sich bis zu 256 Tunnel pro Gateway einrichten.
Name des Tunnels	Dieses Feld enthält den Namen des konfigurierten Tunnels.
Status im IP-Stack	Statusanzeige im IP-Stack. Wertebereich: aktiv / nicht aktiv
Endpunkttyp des lokalen Tunnel	Anzeige der Endpunktadresse auf der Tunnel-Sendeseite (möglich sind die Angabe eines Host- oder DNS-Namens).
Endpunktadresse des lokalen Tunnel	Anzeige der Endpunktadresse im lokalen Tunnel.
Endpunkttyp des Remote Tunnel	Anzeige des Endpunkttyps des Remote-Tunnels.
Endpunktadresse des Remote Tunnel	Anzeige der Empfängeradresse des Remote-Tunnels. Wird die Adresse 0.0.0.0 angezeigt, so bedeutet dies, dass der Tunnelendpunkt unbekannt ist. In diesem Fall muss der Tunnelaufbau immer von der Gegenstelle erfolgen (z.B. Teleworker).
Vorgeschlagene Lebensdauer der Session-Keys	Anzeige der akzeptierten Gültigkeitsdauer für die Sitzungsschlüssel (Session Keys), die verwendet werden. Nach Ablauf dieser Zeit werden keine Daten mehr innerhalb dieser Sitzung ausgetauscht. Als Ersatz für ungültig gewordene Sitzungsschlüssel werden automatisch neue Sitzungsschlüssel ausgehandelt.
Vorgeschlagene Lebensdauer der Schlüsseltausch-Session	Anzeige der akzeptierten Gültigkeitsdauer für die Schlüsseltausch-Session. Nach Ablauf der Schlüsseltausch-Session werden automatisch neue Schlüssel für die Schlüsseltausch-Session durch IKE (Verschlüsselungsprotokoll) ausgehandelt.
Zugehörige Regeln: Zugehörige Senderegel	Einrichtung der Senderegel unter VPN>Regeln
Zugehörige Regeln: Zugehörige Empfangsregel	Einrichtung der Empfangsregel unter VPN>Regeln
Tunneldaten	
Name des Tunnels	Dieses Feld enthält den Namen des konfigurierten Tunnels.
Status im IP-Stack	Statusanzeige im IP-Stack. Wertebereich: aktiv / nicht aktiv
Endpunkttyp des lokalen Tunnel	Anzeige der Endpunktadresse auf der Tunnel-Sendeseite (möglich sind die Angabe eines Host- oder DNS-Namens).
Endpunktadresse des lokalen Tunnel	Anzeige der Endpunktadresse im lokalen Tunnel.
Endpunkttyp des Remote Tunnel	Anzeige des Endpunkttyps des Remote-Tunnels.
Endpunktadresse des Remote Tunnel	Anzeige der Empfängeradresse des Remote-Tunnels. Wird die Adresse 0.0.0.0 angezeigt, so bedeutet dies, dass der Tunnelendpunkt unbekannt ist. In diesem Fall muss der Tunnelaufbau immer von der Gegenstelle erfolgen (z.B. Teleworker).
Regeldaten	
Richtung	

Parameter	Beschreibung
Priorität	Anzeige der Priorität für die Abarbeitungsfolge. Die höchste Priorität wird mit 1 angegeben. Für jede Regel einer Richtung ist eine eigene Priorität zu vergeben. Eine Regel und die dazugehörige Regel der Gegenrichtung müssen stets die gleiche Priorität haben. Die Regel für die Gegenrichtung können Sie nur über den entsprechenden Menüpunkt einrichten.
Aktion für die Regel	Anzeige der IP-Pakete, wie diese mit der Regel zu behandeln sind: pass bedeutet, IP-Pakete werden weitergeleitet, deny bedeutet, es werden keine IP-Pakete weitergeleitet.
Verschlüsselung erforderlich	Anzeige einer Verschlüsselung für diese Regel. Das Verschlüsselungsverfahren wird über den zugeordneten Tunnel definiert.
Regel-Status	
Status im IP-Stack	Statusanzeige im IP-Stack. Wertebereich: aktiv / nicht aktiv
Quelladresse Anzeige der Quell- und Zieladresse in dem Format, das zum gewählten Typ passt. Die Anzeige ist vom gewählten Adresstyp abhängig. Wenn jede beliebige IP-Adresse genutzt werden soll, wird 0.0.0.0 angezeigt. Wird als Zieladresse 0.0.0.0 angegeben, um Pakete in einen Tunnel zu schicken, so muss an der Schnittstelle zum Zielnetzwerk NAT deaktiviert werden. Alternativ ist auch eine IP-Angabe zwischen 0.0.0.1 und 255.255.255.254 möglich, um Pakete in einen Tunnel zu schicken.	
Typ	Anzeige des Typs für die Quelladresse und die Zieladresse (möglich sind: Host, Subnetz, IP Adressbereich und DNS-Name).
Adresse (unterste des Bereichs)	
Subnetzmaske / oberste Adr. des Bereichs	
Zieladresse	
Typ	Anzeige des Typs für die Quelladresse und die Zieladresse (möglich sind: Host, Subnetz, IP Adressbereich und DNS-Name).
Adresse (unterste des Bereichs)	Anzeige der Quell- und Zieladresse in dem Format, das zum gewählten Typ passt. Die Eingabemaske ist vom gewählten Adresstyp abhängig. Wenn jede beliebige IP-Adresse genutzt werden soll, wird 0.0.0.0 angezeigt. Wird als Zieladresse 0.0.0.0 angegeben, um Pakete in einen Tunnel zu schicken, so muss an der Schnittstelle zum Zielnetzwerk NAT deaktiviert werden. Alternativ ist auch eine IP-Angabe zwischen 0.0.0.1 und 255.255.255.254 möglich, um Pakete in einen Tunnel zu schicken.
Subnetzmaske / oberste Adr. des Bereichs	
Dienstdaten Anzeige des Dienstes, welche auf die Verschlüsselung beschränkt wurde. Soll die Verschlüsselung nicht auf einen Dienst beschränkt sein, wählen Sie "Beliebiger Dienst" aus.	
Name des Dienstes	
Quell-Port	Anzeige des Tunnels in Empfangsrichtung, für den diese Regel gilt. Aus diesem Tunnel werden die IP-Pakete, die vom Netz empfangen werden, abgeholt. Wählen Sie Keine Tunnelzuordnung, falls in Empfangsrichtung kein Tunnel zugeordnet werden soll.
Ziel-Port	Anzeige des Tunnels in Senderichtung, für den diese Regel gilt. In diesen Tunnel werden die IP-Pakete, die zum Netz gesendet werden müssen, hineingeschickt. Wählen Sie Keine Tunnelzuordnung, falls in Senderichtung kein Tunnel zugeordnet werden soll.

Parameter	Beschreibung
IP-Protokoll	
Name des Tunnels	Dieses Feld enthält den Namen des neu konfigurierten Tunnels.
Remote-Service über VPN ermöglichen: (aktivierbar über Service-Code)	Dieses Feld ankreuzen, wenn der VPN-Tunnel zur Fernadministration genutzt werden soll.
Endpunkttyp des lokalen Tunnel	Wählen Sie den Typ der Endpunktadresse auf der Tunnel-Sendeseite aus (möglich sind die Angabe eines Host- oder DNS-Namens).
Endpunktadresse des lokalen Tunnel	Tragen Sie die Senderadresse in dem zum Endpunkttyp passenden Format ein.
Endpunkttyp des Remote Tunnel	Typ der Endpunktadresse auf der Tunnel-Empfängerseite (Angabe der IP-Adresse unterstützt).
Endpunktadresse des Remote Tunnel	Empfängeradresse in dem zum Endpunkttyp passenden Format. Wird die Adresse 0.0.0.0 eingestellt, so bedeutet dies, dass der Tunnelendpunkt unbekannt ist. In diesem Fall muss der Tunnelaufbau immer von der Gegenstelle erfolgen (z. B. Teleworker).
Session Key Handhabung	Unter Session-Key-Handhabung wird das Verfahren für den Schlüsselaustausch eingetragen (Automatisch, mit dem IKE-Protokoll).
Vorgeschlagene Verschlüsselungsalgorithmen	Welche Algorithmen dürfen verwendet werden Wertebereich: AES, 3DES
Vorgeschlagene Hash-Algorithmen	Welche Hash-Algorithmen (Prüfalgorithmen) verwendet werden dürfen. Die ausgewählten Algorithmen werden vom Initiator der IKE-Aushandlung angeboten. Wertebereich: MD5, SHA1, SHA2
Vorgeschlagene Lebensdauer der Session-Keys	Gültigkeitsdauer für die Sitzungsschlüssel (Session Keys), die verwendet werden. Nach Ablauf dieser Zeit werden keine Daten mehr innerhalb dieser Sitzung ausgetauscht. Als Ersatz für ungültig gewordene Sitzungsschlüssel werden automatisch neue Sitzungsschlüssel ausgehandelt
Vorgeschlagene Lebensdauer der Schlüsseltausch-Session	Gültigkeitsdauer für die Schlüsseltausch-Session. Nach Ablauf der Schlüsseltausch-Session werden automatisch neue Schlüssel für die Schlüsseltausch-Session durch IKE ausgehandelt
Vorgeschlagene Datenvolumen der Session-Keys	Maximales Datenvolumen für die Sitzungsschlüssel (Session Keys). Nach Überschreiten des Datenvolumens wird automatisch ein neuer Session-Key mittels IKE ausgehandelt. Bei der Auswahl von "unbegrenzt" wird die Datenmenge nicht begrenzt
'Perfect Forward Secrecy' aktivieren	Es wird empfohlen, diese Option immer anzukreuzen, da hiermit ein verbesserter Sicherheitsmechanismus für den Datentransfer über den Tunnel aktiviert wird
Authentifizierungsverfahren für die VPN-Peers	Authentifizierungsverfahren für die VPN-Teilnehmer. Möglich sind digitale Signaturen (Authentifizierung über Zertifikate) und Pre-Shared Keys (Authentifizierung über selbstdefinierte manuelle Schlüssel)
Pre-Shared Key	Dieses Feld ist nur vorhanden, wenn das Authentifizierungsverfahren auf Pre-Shared Keys gesetzt ist. Hier ist das Kennwort einzutragen, das von den VPN-Teilnehmern an beiden Endpunkten des Tunnels verwendet werden muss. Es sollten mindestens 12 Zeichen verwendet werden

Parameter	Beschreibung
Wiederholung des Pre-Shared Key	Dieses Feld ist nur vorhanden, wenn das Authentifizierungsverfahren auf Pre-Shared Keys gesetzt ist.
Liste der CA-Zertifikate	Diese Optionen sind nur vorhanden, wenn das Authentifizierungsverfahren auf Digitale Signaturen gesetzt ist. Die VPN-Teilnehmer können jedes Zertifikat zur Authentifizierung verwenden, dass von einem der angekreuzten CA-Zertifikate ausgestellt (signiert) wurde
Vorgeschlagene Diffie-Hellman-Gruppen	Die VPN-Teilnehmer können jedes angekreuzte Verfahren zum Schlüsselaustausch verwenden

INFO: Das Hinzufügen/Löschen eines VPN-Tunnels muss abschließend unter "VPN > Aktivieren der konfigurierten VPN-Tabellen" aktiviert werden.

27.3.2.18 Sicherheit > VPN > Regeln > Aktive Regeln

Parameterbeschreibung der Registerkarte:

- **Regeln anzeigen**

Parameter	Beschreibung
Priorität	Anzeige der Priorität für die Abarbeitungsfolge als Ziffer. Die höchste Priorität wird mit 1 angegeben. Für jede Regel einer Richtung ist eine eigene Priorität zu vergeben. Eine Regel und die dazugehörige Regel der Gegenrichtung müssen stets die gleiche Priorität haben.
Dienst	Anzeige des Dienstes auf das die Verschlüsselung beschränkt wird. Ist die Verschlüsselung nicht auf einen Dienst beschränkt, so wird "Beliebiger Dienst" angezeigt.
Aktion für die Regel	Anzeige, wie die IP-Pakete mit dieser Regel zu behandeln sind: pass bedeutet, IP-Pakete werden weitergeleitet, deny bedeutet, es werden keine IP-Pakete weitergeleitet.
Verschlüsselung erforderlich	Anzeige der Verschlüsselung. Das Verschlüsselungsverfahren wird über den zugeordneten Tunnel definiert.
Regel-Status	
Status im IP-Stack	Statusanzeige im IP-Stack. Wertebereicht: Aktiviert / Deaktiviert
Quelladresse	
Typ	Anzeige des Typs für die Quelladresse. Wertebereich: Host, Subnetz, IP-Adressbereich, DNS-Name
Adresse (unterste des Bereichs)	
Subnetzmaske / oberste Adr. des Bereichs	
Zieladresse	
Typ	Anzeige des Typs für die Zieladresse. Wertebereich: Host, Subnetz, IP-Adressbereich, DNS-Name

Parameter	Beschreibung
Adresse (oberste des Bereichs)	
Subnetzmaske / oberste Adr. des Bereichs	
Tunnel für die Verschlüsselung	
Tunnel auf der Empfangsseite	Anzeige des Tunnels in Empfangsrichtung, für den diese Regel gilt. Aus diesem Tunnel werden die IP-Pakete, die vom Netz empfangen werden, abgeholt. Anzeige: Keine Tunnelzuordnung (falls in Empfangsrichtung kein Tunnel zugeordnet wurde).
Tunnel auf der Sendeseite	Anzeige des Tunnels in Senderichtung, für den diese Regel gilt. Aus diesem Tunnel werden die IP-Pakete, die vom Netz empfangen werden, abgeholt. Anzeige: Keine Tunnelzuordnung (falls in Senderichtung kein Tunnel zugeordnet wurde).

27.3.2.19 Sicherheit > VPN > Regeln > Konfigurierte Regeln

Regeln legen fest, was mit einem IP-Paket geschehen soll. Die Regelaktion Pass bedeutet, dass das IP-Paket weitertransportiert (durchgelassen) wird. Die Regelaktion Deny bedeutet, dass das IP-Paket nicht weitertransportiert (ignoriert) wird. Es kann jeweils ausgewählt werden, ob das IP-Paket einen (verschlüsselten) VPN-Tunnel benutzt oder nicht. Das Kommunikationssystem kann 640 Regeln verwalten, davon sind 6 Regeln vorbelegt (Default-Regeln) und 634 frei zur Vergabe.

Parameterbeschreibung der Registerkarten:

- **Regeln anzeigen**
- **Regel hinzufügen**
- **Regel ändern**
- **Regel für Gegenrichtung hinzufügen**
- **Regel löschen**

Parameter	Beschreibung
Priorität	Anzeige der Priorität für die Abarbeitungsfolge als Ziffer. Die höchste Priorität wird mit 1 angegeben. Für jede Regel einer Richtung ist eine eigene Priorität zu vergeben. Eine Regel und die dazugehörige Regel der Gegenrichtung müssen stets die gleiche Priorität haben.
Dienst	Anzeige des Dienstes auf das die Verschlüsselung beschränkt wird. Ist die Verschlüsselung nicht auf einen Dienst beschränkt, so wird "Beliebiger Dienst" angezeigt.
Aktion für die Regel	Anzeige, wie die IP-Pakete mit dieser Regel zu behandeln sind: pass bedeutet, IP-Pakete werden weitergeleitet, deny bedeutet, es werden keine IP-Pakete weitergeleitet.
Verschlüsselung erforderlich	Anzeige der Verschlüsselung. Das Verschlüsselungsverfahren wird über den zugeordneten Tunnel definiert.
Regel-Status	
Status im IP-Stack	Statusanzeige im IP-Stack. Wertebereich: Aktiviert / Deaktiviert
Quelladresse	

Parameter	Beschreibung
Typ	Anzeige des Typs für die Quelladresse. Wertebereicht: Host, Subnetz, IP-Adressbereich, DNS-Name
Adresse (unterste des Bereichs)	
Subnetzmaske / oberste Adr. des Bereichs	
Zieladresse	
Typ	Anzeige des Typs für die Zieladresse. Wertebereich: Host, Subnetz, IP-Adressbereich, DNS-Name
Adresse (oberste des Bereichs)	
Subnetzmaske / oberste Adr. des Bereichs	
Tunnel für die Verschlüsselung	
Tunnel auf der Empfangsseite	Anzeige des Tunnels in Empfangsrichtung, für den diese Regel gilt. Aus diesem Tunnel werden die IP-Pakete, die vom Netz empfangen werden, abgeholt. Anzeige: Keine Tunnelzuordnung (falls in Empfangsrichtung kein Tunnel zugeordnet wurde).
Tunnel auf der Sendeseite	Anzeige des Tunnels in Senderichtung, für den diese Regel gilt. Aus diesem Tunnel werden die IP-Pakete, die vom Netz empfangen werden, abgeholt. Anzeige: Keine Tunnelzuordnung (falls in Senderichtung kein Tunnel zugeordnet wurde).

27.3.2.20 Sicherheit > VPN > Public Key Infrastructure (PKI)

Der PKI-Server bezeichnet einen Server, der digitale Zertifikate ausstellen, verteilen und prüfen kann. Die innerhalb einer PKI (Public Key Infrastruktur) ausgestellten Zertifikate werden zur Absicherung der Kommunikation verwendet. Über die vom PKI-Server konfigurierte PKI-URL wird bei Verwendung von Zertifikaten (digitalen Signaturen) versucht, die CRL herunterzuladen.

Parameterbeschreibung der Registerkarten:

- **PKI-Server anzeigen**
- **PKI-Server hinzufügen**

Parameter	Beschreibung
Name des PKI-Servers	Geben Sie einen leicht wiedererkennbaren Namen für den Server ein.
PKI-Servertyp	Wählen Sie die Aufgabe des Servers aus (möglich sind LDAP und Enrollment).
URL des PKI-Servers	Tragen Sie die URL des Servers ein (z. B.: LDAP://139.21.92.144:389).

27.3.2.21 Sicherheit > SSL > Zertifikatsgenerierung

Der Administrationszugriff erfolgt verschlüsselt über HTTPS unter Verwendung des SSL/TLS - Protokolls. Zertifikate dienen zur Authentifizierung der

Verbindung. Standardmäßig wird ein selbstsigniertes Zertifikat verwendet. Zur Erhöhung der Sicherheit kann ein Kundenspezifisches Zertifikat von einer Zertifizierungsstelle (CA) verwendet werden. Das Kommunikationssystem authentifiziert sich gegenüber dem Admin-Client mit Hilfe der im WBM generierten oder importierten Zertifikate. Im Browser kann ein solches Zertifikat als vertrauliches Zertifikat importiert werden, um Warnmeldungen des Browsers beim Verbinden zum SSL-Server zu vermeiden.

Parameterbeschreibung der Registerkarten:

- **CA-Zertifikat generieren**
- **Selbstsigniertes Zertifikat generieren**

Parameter	Beschreibung
Name des Zertifikats	Name des zu generierenden Zertifikats.
Seriennummer des Zertifikats	Seriennummer für das Zertifikat. Die Nummer muss eine positive ganze Zahl sein
Signatur-Algorithmus-Typ	Zu verwendender Signaturalgorithmus Wertebereich: md5RSA, sha1RSA, sha256RSA, sha512RSA
Länge des öffentl. Schlüssels	Wertebereich, Standardwert: 1024, 1536, 2048
Beginn der Zertifikatsgültigkeit (GMT) Ab wann soll das Zertifikat gültig sein. Die Zeitangabe wird als Greenwich Mean Time (GMT) interpretiert.	
Tag, Monat, Jahr, Std., Min., S.	Einheiten für die Zeiteingabe der Zertifikatsgültigkeit
Ende der Zertifikatsgültigkeit (GMT) Bis wann soll das Zertifikat gültig sein. Die Zeitangabe wird als Greenwich Mean Time (GMT) interpretiert	
Tag, Monat, Jahr, Std., Min., S.	Einheiten für die Zeiteingabe der Zertifikatsgültigkeit
Antragsteller Daten zum Zertifikatsantragsteller gemäß den Konventionen des Standards X.509 ein (z. B. im Feld Land (C) DE für Deutschland). Alle vier Felder müssen ausgefüllt werden.	
Land (C)	
Organisation (O)	
Organisationseinheit (OU)	
Allgemeiner Name (CN)	
Alternativer Antragsteller Diese optionale Angabe unterscheidet zwischen Format des DN-Namens (Angaben wie unter Antragsteller) und Anderes Format (z. B. Eintrag einer IP-Adresse). Die Eingabemaske ist von der Auswahl des Formats abhängig.	
Format des DN-Namens	
Anderes Format	
Erweiterung Alternativer Antragstellername	

Parameter	Beschreibung
Alternativer Antragstellername	
CRL-Verteilungspunkt-Typ	
CRL-Verteilungspunkt	Hier kann (optional mit einer URL) die Stelle angegeben werden, von der aus Zertifikatssperrlisten (CRL) verteilt werden

27.3.2.22 Sicherheit > SSL > Zertifikatsverwaltung

Parameterbeschreibung der Registerkarte:

- **Zertifikat aus Datei anzeigen**

Parameter	Beschreibung
PKCS#12-Format	Falls das Zertifikat in einer PKCS#12-Datei gespeichert ist, muss dieses Feld aktiviert sein.
Entschlüsselungskennwort	Wenn das Feld PKCS#12-Format aktiviert wurde, muss in diesem Feld das gleiche Kennwort angegeben sein, das bei der Dateierstellung verwendet wurde.
Datei mit dem Zertifikat	Eingabe von Pfad und den Dateinamen des Zertifikats. Ggf. auf Durchsuchen klicken, um den Speicherort zu definieren.

27.3.2.23 Sicherheit > SSL > Zertifikatsverwaltung > Server-Zertifikate

Parameterbeschreibung der Registerkarten:

- **Zertifikatsanforderung (CSR) generieren**
- **Server-Zertifikat importieren (PKCS#12)**
- **Zertifikat anzeigen**
- **Zertifikat löschen**
- **Zertifikat exportieren (X.509)**
- **Verlängertes Zertifikat importieren (X.509)**
- **Zertifikat aktivieren**

Parameter	Beschreibung
Name der Zertifikatsanforderung	Name des zu generierenden Zertifikats.
Signatur-Algorithmus-Typ	Für dieses Zertifikat zu verwendender Signaturalgorithmus Wertebereich: md5RSA, sha1RSA, sha256RSA, sha512RSA
Länge des öffentl. Schlüssels	Wertebereich: 1024, 1536, 2048
Antragsteller Daten zum Zertifikatsantragsteller gemäß den Konventionen des Standards X.509 (z. B. im Feld Land (C) DE für Deutschland). Alle vier Felder müssen ausgefüllt werden.	
Land (C)	

Parameter	Beschreibung
Organisation (O)	
Organisationseinheit (OU)	
Allgemeiner Name (CN)	
Alternativer Antragsteller Diese optionale Angabe unterscheidet zwischen Format des DN-Namens (Angaben wie unter Antragsteller) und Anderes Format (z. B. Eintrag einer IP-Adresse). Die Eingabemaske ist von der Auswahl des Formats abhängig.	
Format des DN-Namens	
Anderes Format	
Erweiterung alternativer Antragstellername	(optional) Wertebereich, Standardwert: DNS-Name, IP-Adresse, E-Mail-Adresse, Uniform Resource Indicator, Andere
Alternativer Antragstellername	(optional)
Name des Zertifikats	Name des zu importierenden Zertifikats .
Entschlüsselungskennwort	Kennwort, das bei der Dateierstellung verwendet wurde. Wertebereich: 7 bis 32 Zeichen
Datei mit dem Zertifikat	Im Feld **Datei mit dem Zertifikat** kann das gewünschte Zertifikat eingegeben werden oder über das Feld Durchsuchen ausgewählt werden. Zuerst muss der **Fingerabdruck** des Zertifikats angezeigt werden, dann kann es importiert werden.

27.3.2.24 Sicherheit > Web Sicherheit

Parameterbeschreibung der Registerkarte:

- **Web-Zugriffsfilter**

Parameter	Beschreibung
Web-Clients	Nur in Verbindung mit UC Suite: Aktivieren und Deaktivieren des Web-Zugriffs durch Mobiltelefone und mobile Applikationen (myPortal for Mobile/Tablet, myPortal to go, myPortal for OpenStage, Application Launcher und 3rd party Applikationen via Web Service) Info: Nutzung von Web Clients in Verbindung mit UC Smart über Experten-Modus > Applikationen > UC Smart > Grundeinstellungen
Zugriff per HTTPS	Nur verschlüsselte Verbindungen erlaubt.
Zugriff per HTTP	Unverschlüsselte Verbindungen erlaubt.
Anmeldedaten im Endgerät speichern	Wenn aktiviert, müssen Anmeldedaten nicht bei jedem Start der Applikation eingegeben werden

27.3.3 Netzwerkschnittstellen

Unter **Netzwerkschnittstellen** sind Funktionen zusammengefasst, wie z. B. die Konfiguration der einzelnen LAN-Schnittstellen. Die Schnittstellen können unabhängig voneinander konfiguriert werden.

27.3.3.1 Netzwerkschnittstellen > Mainboard > Host-Name

Parameterbeschreibung der Registerkarten:

- **Host-Name ändern**

Parameter	Beschreibung
Host-Name	Host-Name des Kommunikationssystems - frei wählbar. Beispiel: `commsystem` Sind Name und IP-Adresse des Kommunikationssystems in einem DNS-Server hinterlegt, kann eine Namensauflösung erfolgen. Der Name des Kommunikationssystems setzt sich zusammen aus Host-Name und Domänen-Name. Beispiel: `commsystem.mynet.home`

27.3.3.2 Netzwerkschnittstellen > Mainboard > LAN 1 (WAN)

Parameterbeschreibung der Registerkarten:

- **LAN 1-Modus anzeigen**
- **LAN 1-Schnittstelle bearbeiten**
- **ACD bearbeiten**

Parameter	Beschreibung
Internet Service Provider-Auswahl	Auswahl, wie der Zugang zu einem ISP (Internet-Service-Provider) über die WAN-Schnittstelle erfolgen soll.
Internet Service Provider-Auswahl: Nicht konfiguriert oder deaktiviert	Die WAN-Schnittstelle wird nicht genutzt.
Internet Service Provider-Auswahl: LAN-Verbindungstyp TCP/IP	Die WAN-Schnittstelle wird für den Zugang zu einem ISP genutzt, der bereits in einem externen Internet-Router konfiguriert ist. Kommunikationssystem und Internet-Router müssen sich nicht im gleichen LAN-Segment befinden, aber die WAN-Schnittstelle muss mit dem LAN-Segment des Internet-Routers verbunden sein.
Internet Service Provider-Auswahl: T-Online, T-DSL Business, …	Das Kommunikationssystem fungiert als Internet-Router. Die WAN-Schnittstelle wird für den Zugang zu einem vorkonfigurierten ISP genutzt.
Internet Service Provider-Auswahl: Provider-PPPoE	Das Kommunikationssystem fungiert als Internet-Router. Die WAN-Schnittstelle wird für den Zugang zu einem ISP über PPPoE genutzt. PPPoE ist das Protokoll, das am häufigsten von DSL-Modems genutzt wird.
Internet Service Provider-Auswahl: Provider-PPTP	Das Kommunikationssystem fungiert als Internet-Router. Die WAN-Schnittstelle wird für den Zugang zu einem ISP über PPTP genutzt. Diese Variante ist z.B. in Österreich gebräuchlich.

Parameter	Beschreibung
Internetzugang über einen externen Router	Der Zugang zum Internet erfolgt über einen externen Router.
Automatische Adresskonfiguration (mit DHCP)	Ein externer DHCP-Server (evtl. der DHCP-Server des Internet-Routers) weist dem Kommunikationssystem eine IP-Adresse zu.
IP-Adresse des Default Routers übernehmen	Der externe DHCP-Server teilt dem Kommunikationssystem die IP-Adresse des Default-Routers (z.B. Internet-Router) mit.
IP-Adresse des DNS-Servers übernehmen	Der externe DHCP-Server teilt dem Kommunikationssystem die IP-Adresse des DNS-Servers mit.
IP-Adresse des SNTP-Servers übernehmen	Der externe DHCP-Server teilt dem Kommunikationssystem die IP-Adresse des SNTP-Servers mit.
IP-Adresse	IP-Adresse der LAN-Schnitstelle.
Netzmaske	Netzmaske des LAN-Segments.
MAC-Adresse	Anzeige der MAC-Adresse der LAN-Schnittstelle.
Ethernet-Link-Modus	Modus der WAN-Schnittstelle.
Ethernet-Link-Modus: Auto	Automatisches Umschalten zwischen 100 und 1000 Mbit/s sowie Halbduplex- und Vollduplex-Betrieb.
Ethernet-Link-Modus: 100HDX	100 Mbit/s, Halbduplex.
Ethernet-Link-Modus: 100FDX	100 Mbit/s, Vollduplex.
Ethernet-Link-Modus: 1000FDX	1000 Mbit/s, Vollduplex.
Max. Datenpaketlänge (Byte)	Maximale Paketlänge in Byte, die für das IP-Protokoll gelten soll. Wertebereich, Standardwert: 576 - 1500, 1500
Netzwerkaddressübersetzung (NAT)	NAT (Network Adress Translation) ist eingeschaltet. Diese Aufgabe wird meist schon von dem externen Router übernommen.
Bandbreitensteuerung für Sprach-Verbindungen	Dieses Feld aktiviert die Bandbreitensteuerung für Sprach-Verbindungen.
Bandbreite Download	Wert der gesamten Bandbreite in kbit/s für den Download vom ISP.
Bandbreite Upload	Wert der gesamten Bandbreite in kbit/s für den Upload zum ISP.
Bandbreite für Sprach-/Fax-Verbindungen (%)	Prozentangabe für die verfügbare Bandbreite für Sprach-/Fax-Verbindungen. Wertebereich, Standardwert: 0 - 100, 80
IEEE802.1p/q-Tagging	Ist dieses Kontrollkästchen aktiviert, so wird in den Ethernet-Paketen (Layer 2) ein "Type of Service" zur Priorisierung mitgegeben. Die Option ist standardmäßig ausgeschaltet.
IEEE802.1p/q-VLAN-ID	Die ID-Nummer des VLAN, ist anzugeben, falls der verwendete Switch Probleme mit dem Standardwert „0“ hat.
Layer 2-QoS-Klasse	
Signalisierungsdaten	Prioritätsklasse für den Verbindungsaufbau. 0 = geringste Priorisierung / 7= höchste Priorisierung. Wertebereich, Standardwert: 0 - 7, 3

Parameter	Beschreibung
Fax/Modem-Payload	Prioritätsklasse für die Fax- und Modemdaten der IP-Verbindung. 0 = geringste Priorisierung / 7= höchste Priorisierung. Wertebereich, Standardwert: 0 - 7, 5
Netzwerksteuerung	Prioritätsklasse für die Daten der Netzwerksteuerung (z. B. Übermittlung von SNMP-Traps). 0 = geringste Priorisierung / 7= höchste Priorisierung. Wertebereich, Standardwert: 0 - 7, 0
Sprach-Payload	Prioritätsklasse für die Sprachdaten der IP-Verbindung. 0 = geringste Priorisierung / 7= höchste Priorisierung. Wertebereich, Standardwert: 0 - 7, 5
Internet-Zugangsdaten für …	
Anschlusskennung / Benutzername / T-Online-Nummer / Mitbenutzernummer/Suffix / Internetzugangs-Kennung / DSL-Login …	Zugangsdaten des Internet-Service-Providers.
Persönliches Kennwort	Kennwort für den Zugang zum Internet-Service-Provider.
Kennwort Wiederholung	Kennwort für den Zugang zum Internet-Service-Provider.
IP-Parameter	
Partner-IP-Adresse der PPP-Verbindung	IP-Adresse des ISP-Servers, wenn der ISP eine statische IP-Adresse verwendet.
Lokale IP-Adresse der PPP-Verbindung	IP-Adresse, die vom ISP für den Internet-Zugang zugeteilt wurde.
Max. Datenpaketlänge (Byte)	Maximale Paketlänge in Bytes für das IP-Protokoll. Wertebereich, Standardwert: 576 - 1500, 1500
IP-Address-Aushandlung	Auswahl, wie die IP-Adresse zwischen den Verbindungspartnern beim Verbindungsaufbau ausgehandelt werden soll.
IP-Address-Aushandlung: konfigurierte IP-Adresse nutzen	Es ist nur die konfigurierte IP-Adresse möglich.
IP-Address-Aushandlung: jede IP-Adresse akzeptieren	Es wird jede vom Partner vorgeschlagene Adresse akzeptiert.
IP-Address-Aushandlung: neue IP-Adresse anfordern	Es wird bei jedem Verbindungsaufbau eine neue IP Adresse angefordert.
DNS-Abfrage	
Internet-Zugang mit DNS-Abfrage	Der DNS-Server wird automatisch ermittelt.
IP-Adresse des bevorzugten DNS-Servers	Es wird ein spezieller DNS-Server ausgewählt.
Allgemeine PPP-Parameter	
Default-Router	Die hier eingerichtete PPP-Verbindung soll als Routing-Ziel verwendet werden.
IP-Header-Komprimierung	Der TCP-Header wird komprimiert. UDP- und RTP-Header werden immer komprimiert.

Parameter	Beschreibung
LCP-Echo-Anforderung senden	Eine LCP-Echo-Anforderung wird gesendet. Diese Funktion dient der Prüfung, ob die Verbindung noch aktiv ist.
PPP automatisch wieder verbinden	Die PPP-Verbindung wird nach einem Verbindungsabbau automatisch wieder aufgebaut (z. B. bei ISP-Zugang mit Flatrate und Zwangstrennung nach 24 Stunden).
PPTP-Parameter	
Lokale IP-Adresse der Kontrollverbindung	IP-Adresse, die vom ISP für die PPTP-Verbindung zugeteilt wurde.
Partner-IP-Adresse der Kontrollverbindung	IP-Adresse des ISP-Servers für die PPTP-Verbindung.
Partner-Netzmaske für die Kontrollverbindung	Netzmaske, die vom ISP für die PPTP-Verbindung zugeteilt wurde.
Short-Hold	
Short-Hold-Modus	Die Betriebsart „Short Hold“ ist für die PPP-Verbindung eingeschaltet. Die nachfolgende Eingabe sind nur bei eingeschaltetem Short-Hold Modus möglich.
Short-Hold-Zeit (s)	Zeit ohne Datenübertragungen, nach der die PPP-Verbindung getrennt werden soll. Der Short-Hold-Timer wird nur von ausgehenden Paketen getriggert. Wertebereich, Standardwert: 10-9999, 60
Authentifizierung	
PPP-Authentifizierung	PPP-Authentifizierung wird aktiviert. Die Einstellung muss entsprechend den vorgaben des ISP erfolgen.
PPP-Benutzername	Frei wählbarer Benutzername, der bei der Authentifizierung durch PAP oder CHAP verwendet werden soll.
PAP-Authentifizierungsmode	Aktivierung und Art der PAP-Authentifizierung für die PPP-Verbindung: nicht benutzt, PAP-Client, PAP-Host.
PAP-Kennwort	Kennwort für die PAP-Authentifizierung.
CHAP-Authentifizierungsmode	Aktivierung und Art der CHAP-Authentifizierung für die PPP-Verbindung: nicht benutzt, CHAP-Client, CHAP-Host, CHAP-Client und -Host.
CHAP-Kennwort	Kennwort für die CHAP-Authentifizierung.
Datenkomprimierung	
DEFLATE-Datenkomprimierung	Für die Komprimierung von PPP-Datenpaketen mit dem Kompressionsalgorithmus DEFLATE.
COMPRESS-Datenkomprimierung	Für die Komprimierung von PPP-Datenpaketen mit dem Kompressionsalgorithmus COMPRESS.
Addressübersetzung	
NAT	NAT (Network Adress Translation) ist eingeschaltet. Folgende Protokolle werden unterstützt: TCP, UDP und ICMP (nur im passiven Modus).
Address-Mapping	wird laut Herr Naendorf entfallen
Router-Einstellungen	
Dauerverbindung	Abhängig von Tarifmodell kann die Dauerverbindung zum ISP aktiviert oder deaktiviert werden. Bei einem Zeittarif sollte die Dauerverbindung deaktiviert sein, bei einer Flatrate ist die Dauerverbindung zu aktivieren.

Parameter	Beschreibung
Automatisch trennen nach (Sekunden)	Ist die Dauerverbindung deaktiviert (Tarifmodell Zeittarif) wird hier die Zeitdauer der Inaktivität angegeben, nach der die Verbindung getrennt werden soll (z. B. 60 Sekunden). Wertebereich, Standardwert: 10-9999, 60
Zwangstrennung um (Std:Min)	Ist die Dauerverbindung aktiviert (Tarifmodell Flatrate) wird hier die Uhrzeit festgelegt, zu der die Internet-Verbindung getrennt werden soll (z. B. 04:59).
Verbindungszeit	Anzeige der abgelaufenen Verbindungszeit in Tag-Std-Min-Sek.
QoS-Parameter	
Bandbreite Download	Wert der gesamten Bandbreite in kbit/s für den Download vom ISP.
Bandbreite Upload	Wert der gesamten Bandbreite in kbit/s für den Upload zum ISP.
Bandbreitensteuerung für Sprach-Verbindungen	Die Bandbreitenkontrolle verhindert das Überbuchen der verfügbaren Übertragungsraten mit Sprachverbindungen innerhalb einer Multilink-Verbindung, d. h. bei aktivierter Header-Kompression werden maximal 5 Sprachverbindungen über einen B-Kanal zugelassen. Dieses Feld aktiviert die Bandbreitensteuerung für Sprach-Verbindungen. Es werden dabei nur Sprachverbindungen betrachtet, deren Routen im Sprachgateway eingerichtet wurden.
Bandbreite für Sprach-/Fax-Verbindungen (%)	Prozentangabe für die verfügbare Bandbreite für Sprach-/Fax-Verbindungen. Wertebereich, Standardwert: 0 - 100, 80

Parameterbeschreibung der Registerkarten:

- **ACD bearbeiten**

Parameter	Beschreibung
Verbindungszeit	Anzeige der abgelaufenen Verbindungszeit in Tag-Std-Min-Sek.
Erzwinge Wiedereinwahl um	Uhrzeit zu der die Verbindung getrennt und wieder aufgebaut werden soll.
ACD aktivieren	Automatische Trennung aktivieren, um der Trennung der Verbindung durch den ISP zu einem ungünstigen Zeitpunkt zuvorzukommen.

27.3.3.3 Netzwerkschnittstellen > Mainboard > LAN 2

Parameterbeschreibung der Registerkarten:

- **LAN 2 -Schnittstelle bearbeiten**

Parameter	Beschreibung
Internetzugang über einen externen Router	Der Zugang zum Internet erfolgt über einen externen Router.
Schnittstelle aktiviert	Die LAN-Schnittstelle ist aktiviert.
IP-Adresse	IP-Adresse des Kommunikationssystems.
Netzmaske	Netzmaske des LAN-Segments, in dem sich das Kommunikationssystem befindet.
MAC-Adresse	Anzeige der MAC-Adresse des Kommunikationssystems.

Parameter	Beschreibung
Max. Datenpaketlänge (Byte)	Maximale Paketlänge in Byte, die für das IP-Protokoll gelten soll. Wertebereich, Standardwert: 576 - 1500, 1500
Ethernet-Link-Modus	Modus der LAN-Schnittstelle.
Ethernet-Link-Modus: Auto	Automatisches Umschalten zwischen 100 und 1000 Mbit/s sowie Halbduplex- und Vollduplex-Betrieb. In diesen Modus kann das Power-Management aktiviert werden.
Ethernet-Link-Modus: 100HDX	100 Mbit/s, Halbduplex. In diesen Modus kann das Power-Management nicht aktiviert werden.
Ethernet-Link-Modus: 100FDX	100 Mbit/s, Vollduplex. In diesen Modus kann das Power-Management nicht aktiviert werden.
Ethernet-Link-Modus: 1000FDX	1000 Mbit/s, Vollduplex. In diesen Modus kann das Power-Management nicht aktiviert werden.
IEEE802.1p/q-Tagging	Ist dieses Kontrollkästchen aktiviert, so wird in den Ethernet-Paketen (Layer 2) ein "Type of Service" zur Priorisierung mitgegeben. Die Option ist standardmäßig ausgeschaltet.
IEEE802.1p/q-VLAN-ID	Die ID-Nummer des VLAN, ist nur anzugeben, falls der verwendete Switch Probleme mit dem Standardwert „0“ hat.
Layer 2-QoS-Klasse	
Signalisierungsdaten	Prioritätsklasse für den Verbindungsaufbau. 0 = geringste Priorisierung / 7= höchste Priorisierung. Wertebereich, Standardwert: 0 - 7, 3
Fax/Modem-Payload	Prioritätsklasse für die Fax- und Modemdaten der IP-Verbindung. 0 = geringste Priorisierung / 7= höchste Priorisierung. Wertebereich, Standardwert: 0 - 7, 5
Netzwerksteuerung	Prioritätsklasse für die Daten der Netzwerksteuerung (z. B. Übermittlung von SNMP-Traps). 0 = geringste Priorisierung / 7= höchste Priorisierung. Wertebereich, Standardwert: 0 - 7, 0
Sprach-Payload	Prioritätsklasse für die Sprachdaten. 0 = geringste Priorisierung / 7= höchste Priorisierung. Wertebereich, Standardwert: 0 - 7, 5

27.3.3.4 Netzwerkschnittstellen > Mainboard > LAN 3 (Admin)

Parameterbeschreibung der Registerkarten:

- **LAN 3-Schnittstelle bearbeiten**

Parameter	Beschreibung
Schnittstelle aktiviert	Die LAN-Schnittstelle ist aktiviert.
Automatische Adresskonfiguration (mit DHCP)	Ein externer DHCP-Server weist dem Kommunikationssystem eine IP-Adresse zu.
IP-Adresse des Default Routers übernehmen	Der externe DHCP-Server teilt dem Kommunikationssystem die IP-Adresse des Default-Routers (z.B. Internet-Router) mit.

Parameter	Beschreibung
IP-Adresse des DNS-Servers übernehmen	Der externe DHCP-Server teilt dem Kommunikationssystem die IP-Adresse des DNS-Servers mit.
IP-Adresse des SNTP-Servers übernehmen	Der externe DHCP-Server teilt dem Kommunikationssystem die IP-Adresse des SNTP-Servers mit.
IP-Adresse	IP-Adresse der LAN-Schnittstelle.
Netzmaske	Netzmaske des LAN-Segments.
MAC-Adresse	Anzeige der MAC-Adresse der LAN-Schnittstelle.
Ethernet-Link-Modus	Modus der LAN-Schnittstelle.
Ethernet-Link-Modus: Auto	Automatisches Umschalten zwischen 100 und 1000 Mbit/s sowie Halbduplex- und Vollduplex-Betrieb.
Ethernet-Link-Modus: 100HDX	100 Mbit/s, Halbduplex.
Ethernet-Link-Modus: 100FDX	100 Mbit/s, Vollduplex.
Ethernet-Link-Modus: 1000FDX	1000 Mbit/s, Vollduplex.
Max. Datenpaketlänge (Byte)	Maximale Paketlänge in Byte, die für das IP-Protokoll gelten soll. Wertebereich, Standardwert: 576 - 1500, 1500

27.3.3.5 Netzwerkschnittstellen > Mainboard > FTP-Server

Parameterbeschreibung der Registerkarten:

- **FTP-Server Parameter ändern**

Parameter	Beschreibung
FTP-Server freigeben	Ist das Kontrollkästchen aktiviert, ist der interne FTP-Server freigegeben.
Download-Nutzer 'Phone'	
Name	Name für den Zugang der IP-Telefone zum FTP-Server, um aktuelle Software-Updates herunterladen zu können. Der Name kann nicht geändert werden.
Neues Kennwort	Kennwort für den Zugang der IP-Telefone zum FTP-Server. Wird das vordefinierte Kennwort geändert, muss das Kennwort auch an den IP-Telefonen geändert werden.
Kennwort wiederholen	Kennwort für den Zugang der IP-Telefone zum FTP-Server.
Download-Nutzer 'FTP_Admin'	
Name	Name für den Zugang des Administrators zum FTP-Server. Der Name kann nicht geändert werden.
Neues Kennwort	Kennwort für den Zugang des Administrators zum FTP-Server.
Kennwort wiederholen	Kennwort für den Zugang des Administrators zum FTP-Server.

27.3.3.6 Netzwerkschnittstellen > Mainboard > DHCP Modus

Parameterbeschreibung der Registerkarten:

- **DHCP Mode ändern**

Parameter	Beschreibung
kein DHCP	Ist das Optionsfeld aktiviert, ist der interne DHCP-Server ausgeschaltet.
DHCP-Server	Ist das Optionsfeld aktiviert, ist der interne DHCP-Server eingeschaltet.
DHCP-Relay-Agent	Ist das Optionsfeld aktiviert, fungiert das Kommunikationssystem als DHCP-Relay-Agent. Die DHCP-Anfragen der IP-Teilnehmer werden vom Kommunikationssystem an den eigentlichen DHCP-Server weitergeleitet. DHCP-Server und IP-Teilnehmer müssen sich nicht im selben Netzwerksegment befinden.

27.3.3.7 Netzwerkschnittstellen > Mainboard > DHCP Modus > DHCP-Server > Globale Parameter

Die hier aufgeführten netzwerkspezifischen Daten werden vom DHCP-Server an die IP-Teilnehmer übertragen.

Parameterbeschreibung der Registerkarten:

- **Globale Parameter ändern**

Parameter	Beschreibung
DHCP-Server aktivieren	Zeigt an, dass der interne DHCP-Server eingeschaltet ist und seine globalen Parameter konfiguriert werden können. Nicht veränderbar.
Netzmaske	Die Netzmaske definiert die Größe des Subnetzes. Beispiel: `255.255.255.0`.
Broadcast-Adresse	Mit der Broadcast-Adresse können alle IP-Teilnehmer eines Netzes oder Subnetzes vom DHCP-Server angesprochen werden (optional). Beispiel: `0.0.0.0`.
Default Gateway	
Gateway 1	IP-Adresse, unter der das Default Gateway zu erreichen ist. Wird im Netz ein Internet-Router verwendet, ist der Internet-Router das Default Gateway. Beispiel: `192.168.1.1`. Ist das Kommunikationssystem direkt an ein Internet-Modem angeschlossen, ist das Kommunikationssystem das Default Gateway. Beispiel: `192.168.1.2`.
Gateway 2	IP-Adresse, unter der ein zweites Default Gateway (Router) zu erreichen ist (optional).
Gateway 3	IP-Adresse, unter der ein drittes Default Gateway (Router) zu erreichen ist (optional).
DNS Server	
Domänen-Name	Domänen-Name des internen Netzes, max. 80 Zeichen, z. B. `mynet.home` (optional).
Server 1	IP-Adresse, unter der der DNS-Server erreichbar ist. Ist das Kommunikationssystem direkt mit einem Internet-Modem verbunden, muss der Standardwert `0.0.0.0` nicht geändert werden. Das Kommunikationssystem verbindet sich so automatisch mit einem DNS-Server aus dem Internet. Es kann auch ein externer DNS-Server eingetragen werden. Beispiel: der DNS-Server des Internet-Routers (`192.168.1.1)` oder ein DNS-Server aus dem Internet (`google-public-dns-a.google.com`).

Parameter	Beschreibung
Server 2	IP-Adresse, unter der ein zweiter DNS-Server zu erreichen ist (optional).
Server 3	IP-Adresse, unter der ein dritter DNS-Server zu erreichen ist (optional).
Gültigkeitsdauer in Stunden (0 unendlich)	Maximale Gültigkeitsdauer in Stunden, 0 = unendliche Gültigkeitsdauer (Standard: 1 h).
Dynamisch DNS aktualisieren	Ist das Kontrollkästchen aktiviert, wird ein dynamisches Update des DNS-Servers erlaubt. Standard: nicht aktiviert.
Internes DLI verwenden	Ist das Kontrollkästchen aktiviert, wird der interne DLI verwendet. Ist das Kontrollkästchen deaktiviert, erscheinen die Parameter für einen externen DLS-Server. Standard: aktiviert.
Externer DLS Server	
IP-Adresse	IP-Adresse, unter der der externe DLS-Server zu erreichen ist.
Port	Port, unter dem der externe DLS-Server zu erreichen ist.

27.3.3.8 Netzwerkschnittstellen > Mainboard > DHCP Modus > DHCP-Server > IP-Adressen-Pools

Parameterbeschreibung der Registerkarten:

- **IP-Adressen-Pools anzeigen**
- **IP-Adressen-Pool hinzufügen**
- **IP-Adressen-Pool ändern**
- **IP-Adressen-Pool löschen**

Parameter	Beschreibung
Subnetz Adresse	Subnetz-Adresse definiert den maximalen IP-Adressbereich. Beispiel: `192.168.1.0`.
Netzmaske	Die Netzmaske definiert die Größe des Subnetzes. Standard ist `255.255.255.0`.
Adressbereich	
Adressbereich 1	Untere und obere Grenze des IP-Adressbereiches des Subnetzes. Beispiel: von `192.168.1.50` bis `192.168.1.254`.
Adressbereich 2	Untere und obere Grenze eines zweiten IP-Adressbereiches des gleichen Subnetzes (optional).
Adressbereich 3	Untere und obere Grenze eines dritten IP-Adressbereiches des gleichen Subnetzes (optional).
Default Gateway	
Gateway 1	IP-Adresse, unter der das Default Gateway zu erreichen ist. Wird im Netz ein Internet-Router verwendet, ist der Internet-Router das Default Gateway. Beispiel: `192.168.1.1`. Ist das Kommunikationssystem direkt an ein Internet-Modem angeschlossen, ist das Kommunikationssystem das Default Gateway. Beispiel: `192.168.1.2`.
Gateway 2	IP-Adresse, unter der ein zweites Default Gateway (Router) zu erreichen ist (optional).

Parameter	Beschreibung
Gateway 3	IP-Adresse, unter der ein drittes Default Gateway (Router) zu erreichen ist (optional).
Broadcast Adresse	Mit der Broadcast-Adresse können alle IP-Teilnehmer eines Netzes oder Subnetzes vom DHCP-Server angesprochen werden (optional). Standard: `0.0.0.0`.
Domänen Name	Domänen-Name des internen Netzes, max. 80 Zeichen, z. B. `mynet.home` (optional).
DNS Server	
Server 1	IP-Adresse, unter der der DNS-Server erreichbar ist. Ist das Kommunikationssystem direkt mit einem Internet-Modem verbunden, muss der Standardwert `0.0.0.0` nicht geändert werden. Das Kommunikationssystem verbindet sich so automatisch mit einem DNS-Server aus dem Internet. Es kann auch ein externer DNS-Server eingetragen werden. Beispiel: der DNS-Server des Internet-Routers (`192.168.1.1)` oder ein DNS-Server aus dem Internet (`google-public-dns-a.google.com`).
Server 2	IP-Adresse, unter der ein zweiter DNS-Server zu erreichen ist (optional).
Server 3	IP-Adresse, unter der ein dritter DNS-Server zu erreichen ist (optional).
Gültigkeitsdauer in Stunden (0 unendlich)	Maximale Gültigkeitsdauer in Stunden, 0 = unendliche Gültigkeitsdauer (Standard: 1h).

27.3.3.9 Netzwerkschnittstellen > Mainboard > DHCP Modus > DHCP-Server > Statische IP-Adressen

Parameterbeschreibung der Registerkarten:

- **Statische IP Adressen anzeigen**
- **Statische IP Adresse hinzufügen**
- **Statische IP Adresse ändern**
- **Statische IP Adresse löschen**

Parameter	Beschreibung
Rechnername	Name oder Beschreibung des IP-Teilnehmers (z. B. PC oder Server), der eine feste IP-Adresse erhalten soll. Beispiel: `Druckerserver`.
IP-Adresse	Gewünschte feste IP-Adresse. Beispiel: `192.168.1.10`.
Client-Identifizierer	MAC-Adresse des IP-Teilnehmers.
Netzmaske	Netzmaske des Subnetzes. Beispiel: `255.255.255.0`.
Default Gateway	
Standardgateway 1	IP-Adresse, unter der das Default Gateway zu erreichen ist. Wird im Netz ein Internet-Router verwendet, ist der Internet-Router das Default Gateway. Beispiel: `192.168.1.1`. Ist das Kommunikationssystem direkt an ein Internet-Modem angeschlossen, ist das Kommunikationssystem das Default Gateway. Beispiel: `192.168.1.2`.
Standardgateway 1	IP-Adresse, unter der ein zweites Default Gateway (Router) zu erreichen ist (optional).

Parameter	Beschreibung
Standardgateway 1	IP-Adresse, unter der ein drittes Default Gateway (Router) zu erreichen ist (optional).
Broadcast-Adresse	Mit der Broadcast-Adresse können alle IP-Teilnehmer eines Netzes oder Subnetzes vom DHCP-Server angesprochen werden (optional). Beispiel: `0.0.0.0`.
Domänen Name	Domänen-Name des internen Netzes, max. 80 Zeichen, z. B. `mynet.home` (optional).
DNS Server	
Server 1	IP-Adresse, unter der der DNS-Server erreichbar ist. Ist das Kommunikationssystem direkt mit einem Internet-Modem verbunden, muss der Standardwert `0.0.0.0` nicht geändert werden. Das Kommunikationssystem verbindet sich so automatisch mit einem DNS-Server aus dem Internet. Es kann auch ein externer DNS-Server eingetragen werden. Beispiel: der DNS-Server des Internet-Routers (`192.168.1.1)` oder ein DNS-Server aus dem Internet (`google-public-dns-a.google.com`).
Server 2	IP-Adresse, unter der ein zweiter DNS-Server zu erreichen ist (optional).
Server 3	IP-Adresse, unter der ein dritter DNS-Server zu erreichen ist (optional).
Gültigkeitsdauer in Stunden (0 unendlich)	Maximale Gültigkeitsdauer in Stunden, 0 = unendliche Gültigkeitsdauer (Standard: 1 h).

27.3.3.10 Netzwerkschnittstellen > Mainboard > DHCP Modus > DHCP-Server > Zuletzt aktive Leases

Die von einem DHCP-Server zugewiesene IP-Adresse bleibt für einen IP-Teilnehmer so lange gültig wie es die "Lease-Dauer" vorsieht, auch wenn der IP-Teilnehmer zwischenzeitlich ausgeschaltet ist. Hier werden die zuletzt aktiven Zuweisungen angezeigt.

Parameterbeschreibung der Registerkarten:

- **Lease anzeigen**
- **Lease löschen**

Parameter	Beschreibung
IP-Adresse	Vom DHCP-Server zugewiesene IP-Adresse des IP-Teilnehmers.
MAC-Adresse	MAC-Adresse des IP-Teilnehmers, dem eine IP-Adresse zugwiesen wurde.
Client-ID	Client-ID des IP-Teilnehmers. Ist die Client-ID nicht verfügbar, wird die MAC-Adresse des IP-Teilnehmers angezeigt.
Rechnername	Name oder Rufnummer des IP-Teilnehmers, dem eine IP-Adresse zugwiesen wurde.
Start der Lease	Startzeitpunkt der Zuweisung. Der IP-Teilnehmer hat ab diesem Zeitpunkt eine IP-Adresse zugewiesen bekommen.
Ende der Lease	Endzeitpunkt der Zuweisung. Danach startet der IT-Teilnehmer eine neue Anfrage nach einer IP-Adresse.

27.3.3.11 Netzwerkschnittstellen > Mainboard > DHCP Modus > DHCP-Server > Alle Leases

Die von einem DHCP-Server zugewiesene IP-Adresse bleibt für einen IP-Teilnehmer so lange gültig wie es die "Lease-Dauer" vorsieht, auch wenn der IP-Teilnehmer zwischenzeitlich ausgeschaltet ist. Hier werden alle Zuweisungen angezeigt.

Parameterbeschreibung der Registerkarten:

- **Lease anzeigen**
- **Lease löschen**

Parameter	Beschreibung
IP-Adresse	Vom DHCP-Server zugewiesene IP-Adresse des IP-Teilnehmers.
MAC-Adresse	MAC-Adresse des IP-Teilnehmers, dem eine IP-Adresse zugwiesen wurde.
Client-ID	Client-ID des IP-Teilnehmers. Ist die Client-ID nicht verfügbar, wird die MAC-Adresse des IP-Teilnehmers angezeigt.
Rechnername	Name oder Rufnummer des IP-Teilnehmers, dem eine IP-Adresse zugwiesen wurde.
Start der Lease	Startzeitpunkt der Zuweisung. Der IP-Teilnehmer hat ab diesem Zeitpunkt eine IP-Adresse zugewiesen bekommen.
Ende der Lease	Endzeitpunkt der Zuweisung. Danach startet der IT-Teilnehmer eine neue Anfrage nach einer IP-Adresse.

27.3.3.12 Netzwerkschnittstellen > Applicationboard > Host-Name

Parameterbeschreibung der Registerkarten:

- **Host-Name ändern**

Parameter	Beschreibung
Host-Name	Host-Name des Application Boards - frei wählbar. Beispiel: `applboard` Sind Name und IP-Adresse des Application Boards in einem DNS-Server hinterlegt, kann eine Namensauflösung erfolgen. Der Name des Application Boards setzt sich zusammen aus Host-Name und Domänen-Name. Beispiel: `applboard.mynet.home`

27.3.3.13 Netzwerkschnittstellen > Applicationboard > LAN 1

Parameterbeschreibung der Registerkarten:

- **LAN 1-Schnittstelle ändern**

Parameter	Beschreibung
Schnittstelle aktiviert	Ist dieses Kontrollkästchen aktiviert, ist die LAN 1-Schnittstelle des Application Boards aktiv.
Automatische Adresskonfiguration (mit DHCP)	Ist dieses Kontrollkästchen aktiviert, werden der LAN 1-Schnittstelle automatisch vom DHCP-Server die IP-Adresse und die Netzmaske zugewiesen. Zusätzlich kann gewählt werden, ob weitere netzwerkspezifische Parameter vom DHCP-Server übernommen werden.
IP-Adresse des Default Routers übernehmen	Ist dieses Kontrollkästchen aktiviert, wird vom DHCP-Server die IP-Adresse des Default Routers übernommen.
IP-Adresse des DNS-Servers übernehmen	Ist dieses Kontrollkästchen aktiviert, wird vom DHCP-Server die IP-Adresse des DNS-Servers übernommen.
IP-Adresse des SNTP-Servers übernehmen	Ist dieses Kontrollkästchen aktiviert, wird vom DHCP-Server die IP-Adresse des SNTP-Servers übernommen.
IP-Adresse	IP-Adresse, unter der das Application Board zu erreichen ist.
Netzmaske	Netzmaske, unter der das Application Board zu erreichen ist.
MAC-Adresse	MAC-Adresse des Application Boards (nicht editierbar).
Ethernet-Link-Modus	Modus die LAN-Schnittstelle.
Ethernet-Link-Modus: Auto	Automatisches Umschalten zwischen 100 und 1000 Mbit/s sowie Halbduplex- und Vollduplex-Betrieb. In diesen Modus kann das Power-Management aktiviert werden.
Ethernet-Link-Modus: 100HDX	100 Mbit/s, Halbduplex. In diesen Modus kann das Power-Management nicht aktiviert werden.
Ethernet-Link-Modus: 100FDX	100 Mbit/s, Vollduplex. In diesen Modus kann das Power-Management nicht aktiviert werden.
Ethernet-Link-Modus: 1000FDX	1000 Mbit/s, Vollduplex. In diesen Modus kann das Power-Management nicht aktiviert werden.
Max. Datenpaketlänge (Byte)	Maximale Paketlänge in Byte, die für das IP-Protokoll gelten soll. Es sind Werte von 576 bis 1500 erlaubt.

27.3.3.14 Netzwerkschnittstellen > Applicationboard > LAN 2

Parameterbeschreibung der Registerkarten:

- **LAN 2-Schnittstelle ändern**

Parameter	Beschreibung
Schnittstelle aktiviert	Ist dieses Kontrollkästchen aktiviert, ist die LAN 2-Schnittstelle des Application Boards aktiv.
IP-Adresse	IP-Adresse, unter der das Application Board zu erreichen ist.
Netzmaske	Netzmaske, unter der das Application Board zu erreichen ist.
MAC-Adresse	MAC-Adresse des Application Boards (nicht editierbar).
Max. Datenpaketlänge (Byte)	Maximale Paketlänge in Byte, die für das IP-Protokoll gelten soll. Es sind Werte von 576 bis 1500 erlaubt.

Parameter	Beschreibung
Ethernet-Link-Modus	Modus die LAN-Schnittstelle.
Ethernet-Link-Modus: Auto	Automatisches Umschalten zwischen 100 und 1000 Mbit/s sowie Halbduplex- und Vollduplex-Betrieb. In diesen Modus kann das Power-Management aktiviert werden.
Ethernet-Link-Modus: 100HDX	100 Mbit/s, Halbduplex. In diesen Modus kann das Power-Management nicht aktiviert werden.
Ethernet-Link-Modus: 100FDX	100 Mbit/s, Vollduplex. In diesen Modus kann das Power-Management nicht aktiviert werden.
Ethernet-Link-Modus: 1000FDX	1000 Mbit/s, Vollduplex. In diesen Modus kann das Power-Management nicht aktiviert werden.
IEEE802.1p/q-Tagging	Ist dieses Kontrollkästchen aktiviert, wird das Ethernet-Format festgelegt, das vom Application Board gesendet wird. Die Option ist standardmäßig ausgeschaltet.
IEEE802.1p/q-VLAN-ID	ID-Nummer des VLAN, die vom Standardwert „0“ abweicht, falls der verwendete Switch Probleme mit dem Standardwert „0“ hat.
Layer 2-QoS-Klasse	
Signalisierungdaten	Prioritätsklasse für den Verbindungsaufbau. 0 = geringste Priorisierung / 7= höchste Priorisierung .
Fax/Modem-Payload	Prioritätsklasse für für die Fax- und Modemdaten der IP-Verbindung. 0 = geringste Priorisierung / 7= höchste Priorisierung .
Netzwerksteuerung	Prioritätsklasse für für die Daten der Netzwerksteuerung (z. B. Übermittlung von SNMP-Traps). 0 = geringste Priorisierung / 7= höchste Priorisierung .
Sprach-Payload	Prioritätsklasse für für die Sprachdaten der IP-Verbindung. 0 = geringste Priorisierung / 7= höchste Priorisierung .

27.3.4 Routing

Unter **Routing** werden die Routing-Tabellen verwaltet. In kleinen Netzen kann eine Routing-Tabelle auf jedem Router vom Administrator manuell gepflegt werden. In größeren Netzen wird diese Aufgabe mithilfe eines Protokolls automatisiert, das Routing-Informationen im Netz verteilt.

27.3.4.1 Routing > IP-Routing > Mainboard > Statische Routen

Das Kommunikationssystem unterstützt ausschließlich statische Routen. Statische Routen verbinden zwei IP-Geräte miteinander. Sie werden manuell angelegt.

Je nach Applikation ist es ggf. nötig, für das System (Mainboard) und die UC Booster Card (Application Board) unterschiedliche Routen einzustellen.

Parameterbeschreibung der Registerkarten:

- **Statische Routentabelle anzeigen**
- **Statische Route hinzufügen**
- **Statische Route ändern**
- **Statische Route löschen**

Parameter	Beschreibung
Route-Index	Der Route-Index wird automatisch vergeben und nur zu Ihrer Information angezeigt. Er kann nicht geändert werden.
Route-Name	Name oder Beschreibung der statischen Route, frei wählbar.
Ziel-Netzwerk/Host	IP-Adresse des Zielnetzes.
Netzmaske	Subnetzmaske des Zielnetzes.
Route-Gateway	IP-Adresse des nächsten Routers auf dieser Route oder IP-Adresse der lokalen oder entfernten Schnittstelle eines PSTN-Partners.

27.3.4.2 Routing > IP-Routing > Mainboard > Default Router

Je nach Applikation ist es ggf. nötig, für das System (Mainboard) und die UC Booster Card (Application Board) ein unterschiedliches Default-Routing einzustellen.

Parameterbeschreibung der Registerkarten:

- **Default Router ändern**

Parameter	Beschreibung
Default-Routing über	IP-Routing über einen Default Router aktivieren oder deaktivieren.
Keine Schnittstelle	IP-Routing über einen Default Router deaktiviert.
LAN	IP-Routing über einen Default Router aktiviert.
IP-Adresse des Default Routers	IP-Adresse des Default Routers, sofern im Feld **Default Routing über** als Schnittstelle **LAN** ausgewählt ist. Beispiel: IP-Adresse des Internet-Routers, `192.168.1.1`.

27.3.4.3 Routing > IP-Routing > Mainboard > DNS-Server

Sie können die IP-Adresse des DNS-Servers anzeigen und gegebenenfalls ändern. Die Einstellung ist für Trunking mit dynamischen IP-Adressen notwendig.

Parameterbeschreibung der Registerkarten:

- **DNS-Einstellungen ändern**

Parameter	Beschreibung
IP-Adresse des DNS-Servers	IP-Adresse, unter der der DNS-Server erreichbar ist. Ist das Kommunikationssystem direkt mit einem Internet-Modem verbunden, muss der Standardwert `0.0.0.0` nicht geändert werden. Das Kommunikationssystem verbindet sich so automatisch mit einem DNS-Server aus dem Internet. Es kann auch ein externer DNS-Server eingetragen werden. Beispiel: der DNS-Server des Internet-Routers (`192.168.1.1)` oder ein DNS-Server aus dem Internet (`google-public-dns-a.google.com`).

27.3.4.4 Routing > IP-Routing > Applicationboard > Statische Routen

Je nach Applikation ist es ggf. nötig, für das System (Mainboard) und die UC Booster Card (Application Board) unterschiedliche Routen einzustellen.

Parameterbeschreibung der Registerkarten:

- **Statische Richtungstabelle anzeigen**
- **Statische Richtung hinzufügen**
- **Statische Richtung ändern**
- **Statische Richtung löschen**

Parameter	Beschreibung
Route-Index	Der Route-Index wird automatisch vergeben und nur zur Information angezeigt. Er kann nicht geändert werden.
Route-Name	Name oder Beschreibung der statischen Route, frei wählbar (optional) Wertebereich: max. 35 Zeichen
Ziel-Netzwerk/Host	IP-Adresse des Zielnetzes.
Netzmaske	Subnetzmaske des Zielnetzes.
Route-Gateway	IP-Adresse des nächsten Routers auf dieser Route oder IP-Adresse der lokalen oder entfernten Schnittstelle eines PSTN-Partners.

27.3.4.5 Routing > IP-Routing > Applicationboard > Default Router

Je nach Applikation ist es ggf. nötig, für das System (Mainboard) und die UC Booster Card (Application Board) ein unterschiedliches Default-Routing einzustellen.

Parameterbeschreibung der Registerkarten:

- **Standard-Router ändern**

Parameter	Beschreibung
Default-Routing über	IP-Routing über einen Default Router aktivieren oder deaktivieren.
Keine Schnittstelle	IP-Routing über einen Default Router deaktiviert.
LAN	IP-Routing über einen Default Router aktiviert.
IP-Adresse des Default Routers	IP-Adresse des Default Routers, sofern im Feld Default Routing über als Schnittstelle LAN ausgewählt ist.

27.3.4.6 Routing > NAT

Sie können eine NAT-Regel für die Netzwerk-Adressübersetzung anzeigen, hinzufügen, ändern und löschen. Über den NAT-Tabelleneditor können Sie bequem alle vorhandenen und weitere NAT-Einträge für die Netzwerk-Adressübersetzung auf einmal bearbeiten.

Parameterbeschreibung der Registerkarten:

- **NAT hinzufügen**
- **NAT Tabelleneditor**

Parameter	Beschreibung
NAT-Regel aktiv	
Beschreibung	
Lokale IP-Adresse	Lokale Zieladresse im LAN.
Lokaler Port	Lokale Port-Nummer des eingestellten Protokolls im LAN.
Globaler Port	Port-Nummer des eingestellten Protokolls.
Protokoll	Zu verwendendes Transportprotokoll. Das eingestellte Transportprotokoll gilt sowohl für die lokalen als auch für die globalen Adress-Angaben.
Protokoll: **TCP**	TCP (Transmission Control Protocol) TCP ist ein zuverlässiges, verbindungsorientiertes Protokoll für die Übertragung von IP-Paketen. Vor Übertragungsbeginn wird ein virtueller Kanal zwischen den beiden Endpunkten der Netzwerkverbindung aufgebaut. Auf diesem Kanal können in beide Richtungen Daten übertragen werden. TCP wird hauptsächlich in den Bereichen WorldWideWeb, E-Mail und Peer-to-Peer-Netzwerke eingesetzt. Zusätzlich wird es auch für die Rufsignalisierung bei der IP-Telefonie verwendet, da es die Eigenschaft besitzt, dass Datenverluste bei der Übertragung erkannt und automatisch behoben werden.
Protokoll: **UDP**	UDP (User Datagram Protocol) UDP ist ein einfaches, verbindungsloses Protokoll für die Übertragung von IP-Paketen. Vor Übertragungsbeginn wird kein virtueller Kanal wie bei TCP zur Gegenstelle aufgebaut, wodurch die PCs schneller mit dem Datenaustausch beginnen können. Zur Adressierung der Sprachpakete wird bei UDP die Portnummer des Dienstes mitgesendet, der die Daten erhalten soll. Es wird hauptsächlich im Bereich DNS und für die Sprachübertragung bei der IP-Telefonie eingesetzt. Da bei einem verbindungslosen Protokoll allerdings nicht kontrolliert wird, ob die Gegenstelle die Daten auch wirklich erhalten hat, kann dies zu Verlusten bei der Sprachübertragung führen.

27.3.4.7 Routing > PSTN

Mit diesen Parametern wird eine IP-Remote-Verbindung (DFÜ-Verbindung) über das klassische Telefonnetz eingerichtet.

Parameterbeschreibung der Registerkarten:

- **Globale PSTN-Daten ändern**

Parameter	Beschreibung
Router-Rufnummer (interne Rufnummer)	Durchwahl des Systems auswählen. Alle Anwendungen, die die Routerfunktion nutzen, sind unter dieser Durchwahl von außen erreichbar. Externe Routingpartner, die keine Rufnummer übermitteln, müssen jeweils andere Rufnummern benutzen. Diese Rufnummern werden als MSN konfiguriert.
Wahlwiederholung	
Anzahl Wahlwiederholungen	Wiederholungsversuche, die das System zum Aufbau einer Verbindung unternehmen soll. Wertebereich: 0 bis 255
Wahlwiederholungspause (s)	Pause zwischen den Wahlwiederholungen in Sekunden. Wertebereich: 1 - 1.000
Scripting	
Kennung 1 für Scripting	Erster Teil der Kennung für die Anmeldung bei Internet-Providern. Der Internet-Provider fordert Einträge zu Host, Nutzer-Identifikation und ein Kennwort, z.B. Host=ERT005, Nutzer=KJUMBERT, Kennwort=123456. Die Einträge lauten folglich: Kennung 1 für Scripting: HOST:ERT005 - Kennung 2 für Scripting: USER:KJUMBERT - Neues Kennwort für Scripting: PASSWORD:123456.
Kennung 2 für Scripting	Zweiter Teil der Kennung für die Anmeldung bei Internet-Providern.
Neues Kennwort für Scripting	Kennwort für die Anmeldung bei Internet-Providern.

27.3.4.8 Routing > PSTN > PPP-Protokoll

Parameterbeschreibung der Registerkarten:

- **Laden über HTTP**

Parameter	Beschreibung
Laden	Das PPP-Logfile kann über HTTP geladen werden. Je nach Einstellung des Browsers wird angezeigt, ob das heruntergeladene Logfile gespeichert oder im Default-Editor geöffnet werden soll.

27.3.4.9 Routing > PSTN > PSTN-Partner

Parameterbeschreibung der Registerkarten:

- **PSTN-Partner hinzufügen**
- **PSTN-Partner anzeigen**
- **PSTN-Partner ändern**

Parameter	Beschreibung
Name des Partners	Name des PSTN-Partners. Folgende PSTN-Partner stehen zur Verfügung: • Default PSTN - nicht konfigurierbar • PSTN Partner 1: Default für CLA, Funktion umkonfigurierbar • PSTN Partner 2: Default für ISDN, Funktion umkonfigurierbar • PSTN Partner 3: Name und Funktion frei konfigurierbar • PSTN Partner 4: Name und Funktion frei konfigurierbar Wertebereich: 1 bis 14 Zeichen
Art der PSTN-Verbindung	Einrichtung der PSTN-Verbindung (Standardauswahl: Aktiv).
Art der PSTN-Verbindung: Nicht konfiguriert	PSTN-Partner kann vorkonfiguriert werden. Ein Verbindungsaufbau über diesen PSTN-Partner wird mit dieser Einstellung jedoch verhindert.
Art der PSTN-Verbindung: Aktiv	PSTN-Partner ist aktiviert. Ein Verbindungsaufbau über diesen PSTN-Partner wird mit dieser Einstellung erlaubt.
Art der PSTN-Verbindung: DSL Fallback	Nutzung des DSL-Zugangs für die PSTN-Verbindung (Default Router ist der DSL-Zugang)
IP-Parameter	
IP-Adresse des PSTN-Partners	IP-Adresse des Host-PC auf der Gegenseite, zu dem die PSTN-Verbindung aufgebaut wird.
IP-Adresse der lokalen PSTN-Schnittstelle	IP-Adresse des lokalen Kommunikationssystems, die für die PSTN-Verbindung benutzt werden soll.
Max. Datenpaketlänge (Byte)	Maximale IP-Paketlänge in Bytes für die PSTN-Verbindung. Wertebereich: 80 bis 1500
IP-Address-Aushandlung	Aushandlung der IP-Adresse zwischen den Verbindungspartnern beim Verbindungsaufbau.
IP-Address-Aushandlung: konfigurierte IP-Adresse nutzen	Nur die konfigurierte IP-Adresse des PSTN-Partners wird akzeptiert.
IP-Address-Aushandlung: jede IP-Adresse akzeptieren	keine IP-Adress-Aushandlung
IP-Address-Aushandlung: neue IP-Adresse anfordern	IP-Adresse wird ausgehandelt
Allgemeine PPP-Parameter	
Default-Router	Der hier eingerichtete PSTN-Partner soll nicht nur vorkonfiguriert, sondern als Routing-Ziel verwendet werden. Es kann nur einen Default-Router geben. Entweder ist dies ein DSL-Zugang oder der hier eingerichtete PSTN-Partner.
Internet-Zugang mit DNS-Abfrage	Der Zugang soll als Internetzugang benutzt werden. Es darf nur ein Internetzugang pro System aktiviert werden darf (entweder ein PSTN-Partner oder ein DSL-Zugang).

Parameter	Beschreibung
Service-Eintrag	Bei einem Ruf zur MSN des PSTN-Partners soll die Rufnummernüberprüfung ausgeschaltet sein. Der Service-Eintrag kann nur aktiviert werden, wenn der PSTN-Partner eine MSN-Nummer hat und eine PAP- oder CHAP-Authentifizierung aktiviert wurde.
MSN/Durchwahl (interne Rufnummer)	Konfiguration der MSN-Nummer. Übermittelt der Partner seine Rufnummer, so muss diese konfiguriert sein, sonst wird der Ruf abgewiesen. Sind hingegen Rufnummern des Partners konfiguriert, aber der Partner übermittelt keine, so kommt die Verbindung trotzdem zustande.
B-Kanäle	Anzahl der verwendeten B-Kanäle. Wertebereich: 1 oder 2
Rückruf	Ein Anruf wird abgelehnt und der Partner danach sofort zurückgerufen. Dies verhindert das Einwählen von nicht autorisierten Gegenstellen. Die anrufende Stelle muss im D-Kanal der ISDN-Verbindung die Rufnummer übertragen und die Einwahl durch das System erlauben. Beim PSTN-Partner muss diese Rufnummer mit gehender Richtung konfiguriert sein. Ist "Rückruf" aktiviert, werden nur gehende Verbindungen von diesem Partner akzeptiert. Ist die Gegenstelle ebenfalls ein Gateway, und ist für diese Verbindung ebenfalls "Rückruf" aktiviert, kann keine Verbindung aufgebaut werden, weil keiner der Partner einen einkommenden Verbindungsaufbau akzeptiert. Ist bei einer solchen Fehlkonfiguration nur "Rückruf ohne Wahlwiederholung" aktiviert, so kann sie erkannt werden, und ein ständiger Verbindungsaufbau wird unterdrückt. Ist jedoch Wahlwiederholung aktiviert, wird das Problem nicht erkannt.
V.34-Gegenstelle	Akzeptieren einer V.34-Gegenstelle (z. B. ein Modem).
PPP automatisch wieder verbinden	PPP Verbindung wird nach einem Verbindungsabbau automatisch wieder aufgebaut (z. B. bei ISP-Zugang mit Flat-Rate und Zwangstrennung nach 24 Stunden).
LCP-Echo-Anforderung senden	Ein LCP Echo-Request wird gesendet. Diese Funktion dient der Prüfung, ob die Verbindung noch aktiv ist.
Short-Hold	
Short-Hold-Modus	Die Betriebsart „Short Hold“ ist für die PPP-Verbindung eingeschaltet. Die nachfolgenden Eingaben sind nur bei eingeschaltetem Short-Hold Modus möglich.
Short-Hold-Zeit (s)	Zeit ohne Datenübertragungen, nach der die PPP-Verbindung getrennt werden soll. Der Shor-t-Hold-Timer wird nur von ausgehenden Paketen getriggert. Wertebereich: 10 bis 9999
Short-Hold-Gebührentaktauswertung	Optimierung des Short-Hold-Betriebs unter Berücksichtigung des Gebührentaktes. Für Anrufe über PPP erfolgt eine Gebührentaktauswertung (Auswertung der Facility Meldungen mit AoC-Info-Elementen). Werden vom Internet-Service-Provider keine Gebühreneinformationen geliefert, so wird als Default-Timeout-Wert 0 Sekunden verwendet.
Authentifizierung	
PPP-Authentifizierung	PPP-Authentifizierung wird aktiviert.
PPP-Benutzername	Frei wählbarer Benutzername, der bei der Authentifizierung durch PAP oder CHAP verwendet werden soll.
PAP-Authentifizierungsmode	Aktivierung und Art der PAP-Authentifizierung für die PPP-Verbindung: nicht benutzt, PAP-Client, PAP-Host.
PAP-Kennwort	Kennwort für die PAP-Authentifizierung.
CHAP-Authentifizierungsmode	Aktivierung und Art der CHAP-Authentifizierung für die PPP-Verbindung: nicht benutzt, CHAP-Client, CHAP-Host, CHAP-Client und -Host.

Parameter	Beschreibung
CHAP-Kennwort	Kennwort für die CHAP-Authentifizierung.
Header-Komprimierung	
IP-Header-Komprimierung	Die Komprimierung des IP/TCP bzw. IP/UDP/RTP-Header ist aktiviert. Die Header-Komprimierung verbessert die Datenübertragung in Voice-over-PPP-Szenarien. Es werden alle Voice-Pakete komprimiert, deren UDP-Portnummern im eingestellten Bereich liegen.
Datenkomprimierung	
DEFLATE-Datenkomprimierung	Komprimierung mit dem DEFLATE-Algorithmus
COMPRESS-Datenkomprimierung	Komprimierung mit dem COMPRESS-Algorithmus
Addressübersetzung	
NAT	NAT (Network Adress Translation) ist eingeschaltet. Folgende Protokolle werden unterstützt: TCP, UDP und ICMP (nur im passiven Modus).
Address-Mapping	Adress-Mapping ist aktiviert.
QoS-Parameter der Schnittstelle	
Bandbreitensteuerung für Sprach-Verbindungen	Die Bandbreitenkontrolle verhindert das Überbuchen der verfügbaren Übertragungsraten mit Sprachverbindungen innerhalb einer Multilink-Verbindung, d. h. bei aktivierter Header-Kompression werden maximal 5 Sprachverbindungen (G.729 / 60ms o. G.723 / 60ms) über einen B-Kanal zugelassen. Dieses Feld aktiviert die Bandbreitensteuerung für Sprach-Verbindungen. Es werden dabei nur Sprachverbindungen betrachtet, deren Routen im Sprachgateway eingerichtet wurden.
Bandbreite für Sprach-/Fax-Verbindungen (%)	Prozentangabe für die verfügbare Bandbreite für Sprach-/Fax-Verbindungen. Wertebereich, Standardwert: 0 - 95, 80

Parameterbeschreibung der Registerkarten:

- **Auf Lieferzustand zurücksetzen**

Parameter	Beschreibung
Übernehmen	Die Werte für den gewählten PSTN-Partner werden auf die Lieferzustandswerte zurückgesetzt.

Parameterbeschreibung der Registerkarten:

- **Rufnummer hinzufügen**
- **Rufnummer ändern**
- **Rufnummer löschen**

Parameter	Beschreibung
Rufnummer	Rufnummer, unter der ein PSTN-Partner erreichbar ist. Sie muss innerhalb der Gesamtkonfiguration eindeutig sein und kann aus bis zu 22 Dezimalziffern (0 bis 9) bestehen. Es können Bindestriche verwendet werden. Zu jedem PSTN-Partner können bis zu fünf Rufnummern konfiguriert werden. Bei Übermittlung der Rufnummer wird diese überprüft und es werden nur Anrufe entgegengenommen, wenn für die eingehende Rufnummer ein PSTN-Partner mit der entsprechenden Rufberechtigung definiert ist.
Rufrichtung	Zustandekommen der Verbindung unter der oben eingetragenen Rufnummer.
Rufrichtung: Gesperrt	Die Nummer ist nicht verwendbar.
Rufrichtung: Kommend	Der Partner darf anrufen, aber nicht angerufen werden.
Rufrichtung: Gehend	Der Partner darf angerufen werden, aber nicht anrufen.
Rufrichtung: Kommend und gehend	Der Partner darf angerufen werden und kann anrufen.
Löschen	Die gewählte Rufnummer wird gelöscht.

27.3.5 LCR

Unter **LCR** werden die Funktionen für LCR wie Berechtigungen, Wahlpläne, Wegetabellen und Wahlregeln zusammengefasst.

27.3.5.1 LCR > LCR-Flags

Parameterbeschreibung der Registerkarte:

- **LCR Flags ändern**

Parameter	Beschreibung
LCR Flags	
LCR freigeben	LCR wird freigegeben und somit die automatische Wegesuche aktiviert.
***!Reset LCR data**	
***!Delete the configured LCR data and initialize the LCR with OSBiz default data**	Wird dieses Optionsfeld aktiviert, werden die konfigurierten LCR-Einträge (Wahlpläne, Wegetabellen, Wahlregeln) gelöscht und durch die Standard-Einträge ersetzt.

INFO: Bei Fehlkonfiguration im LCR besteht die Gefahr, dass gehende Verbindungen nicht oder nur eingeschränkt möglich sind.

27.3.5.2 LCR > Classes Of Service

Parameterbeschreibung der Registerkarte:

- **LCR Berechtigungen ändern**

Parameter	Beschreibung
Index	Hierarchische Indexliste
Rufnummer	Rufnummer des Teilnehmers
Name	Name des Teilnehmers
Berechtigungsgruppe	Jeder Teilnehmer wird einer LCR-Berechtigunggruppe (Class Of Service COS) zugewiesen. Standardmäßig sind alle Teilnehmer mit maximaler LCR-Berechtigung (15) eingetragen Wertebereich: 1 bis 15

INFO: Ein Teilnehmer kann einen Weg nur dann belegen, wenn seine Berechtigung größer oder gleich der LCR-Berechtigung in der Wegetabelle ist.

27.3.5.3 LCR > Wahlplan

Parameterbeschreibung der Registerkarten:

- **Wahlplan ändern**
- **Wahlplan anzeigen**

Parameter	Beschreibung
Wahlplan	Im Wahlplan wird nach Mustern gesucht, die auf die gewählten Ziffern zutreffen. Das Ergebnis dient als Kriterium für die Auswahl der Wegetabelle. Dabei wird ebenfalls überprüft, ob die Berechtigung des Teilnehmers für diese Richtung zutrifft. Für Externverbindungen wird jede Rufnummer einschließlich der Kennzahl (bis max. zur 24 Zeichen incl. Feldtrennzeichen) im Wahlplan überprüft. Der Wahlplan ermittelt dann für den Teilnehmer eine Wegetabelle, die der Teilnehmer für den Verbindungsaufbau zugewiesen bekommt. Über die Wegetabelle werden Wege (Routen) angelegt. Die Wahlregeltabelle legt fest, wie die vom Teilnehmer ausgesuchten Ziffern umgesetzt und vom Kommunikationssystem gewählt werden.
Name	Über die Spalte Name kann jedem Profil wie z. B. Ortsgespräch, Ferngespräch, Ausland ein Name zugeordnet werden. Ob die Spalte Name angezeigt wird, hängt von der jeweiligen Version des Kommunikationssystem ab. Für den Namen sollte ein sprechender Name gewählt werden. Eine Name darf auch mehrfach verwendet werden. Über den Rufnummern-Assistenten werden automatisch entsprechende Namen vergeben.
Gewählte Ziffern	Anhand dieses Schemas wird die Rufnummer ausgewertet, um in die entsprechende Wegetabelle zu verzweigen. Es können die Feldtrennzeichen C und - sowie die Platzhalter X, N und Z verwendet werden. 0...9 feste Ziffern - Feldtrennzeichen (Auswertung durch die Wahlregel) X Platzhalter für eine Ziffer zwischen 0...9 N Platzhalter für eine Ziffer zwischen 2...9 Z Platzhalter für eine oder mehrere Ziffern bis Wahlende C simulierter Wählton (kann max. 3 mal eingetragen werden)

Parameter	Beschreibung
Wegetabelle	In der Spalte Wegetabelle wird angegeben, welche Wegetabelle für das Profil verwendet werden soll. Der Pfeil verlinkt zur Definition der jeweiligen Wegetabelle. Wertebereich: 1 bis 254, davon 1 bis 15 vorbelegt
PKZ	In dieser Spalte wird über Ankreuzen entschieden, ob eine erzwungene PKZ-Eingabe nach der Belegungskennzahl erfolgen soll oder nicht (in USA: nach Wahlende). Wenn nicht ausgewählt, wird die PKZ erst nach der kompletten Wahl des Wahlplans angefordert, wenn dies für die Richtung eingerichtet ist.
Wahlkontrolle	Wenn markiert, dann unterliegen die gewählten Ziffern der Wahlkontrolle (Berechtigung). Dies gilt sowohl für die Vernetzung, als auch für standalone Kommunikationssysteme. Damit können einzelne Rufnummern von der Wahlkontrolle ausgenommen werden. Wenn die Wahlkontrolle durchgeführt werden soll, so gelten die bekannten Regeln über die Verbots- und Erlaubnislisten.
Notbetrieb	Wenn eine hier als Notrufnummer eingerichtete Nummer (Spalte Notbetrieb angekreuzt) angewählt wird und es keine freie Leitung gibt, dann wird eine nicht als Notrufnummer benutzte Leitung (Spalte Notbetrieb nicht angekreuzt) getrennt und diese dann automatisch für den Notruf bereitgestellt.

27.3.5.4 LCR > Wegetabelle

Parameterbeschreibung der Registerkarten:

- **Wegetabelle ändern**

Parameter	Beschreibung
Wegetabellen	Den im Wahlplan definierten Rufnummern wird über die Wegetabellen hier eine Aktion (Wahl) zugeordnet. Wertebereich: 254 Wegetabellen
Index	Die Wegetabelle wird von oben nach unten in hierarchischer Reihenfolge durchsucht. Es wird jeweils überprüft, ob die Richtung frei ist bzw. der Teilnehmer die erforderliche LCR-Berechtigung hat. Ist dies der Fall, erfolgt die Wahl gemäß der in der Wegetabelle eingetragenen Wahlregel. Wertebereich: 1 bis 16
Richtung	Die zu belegende Richtung, siehe "Leitungen/Vernetzung > Richtungen" Standardwert: im System konfigurierter Richtungsnamen
Wahlregel	Durch die LCR-Wahlregeln können eingegebene Rufnummern zur Weiterverarbeitung in beliebige neue Ziffernfolgen umgewandelt werden. Durch Ziffernumwandlung wird der Zugang zu verschiedenen Netzanbietern ermöglicht. Definition unter "Wahlregel". Wertebereich: 254 Wahlregeln
min. Ber.	Die min. Berechtigung beschreibt die LCR-Berechtigung, die ein Teilnehmer mindestens haben muss, um die zugehörige Route verwenden zu dürfen. Hier lässt sich z. B. festlegen, dass ein Teilnehmer nur über einen bestimmten Carrier oder nur zu bestimmten Zeiten telefonieren darf, während andere Teilnehmer eine Ausweichmöglichkeit auf andere Routen erhalten. Der Wert für die maximale Berechtigung ist 15. Wertebereich: 1 bis 15

Parameter	Beschreibung
Warnung	Wenn der primäre Verbindungsweg in der Wegetabelle belegt ist, wird LCR den nächsten (möglicherweise kostspieligeren) in der Tabelle konfigurierten Weg wählen. Dies kann dem Anwender durch ein akustisches und/oder optisches Signal angezeigt werden. Wertebereich: Keine, Ton, Display, Display + Ton
Dediziertes Gateway	Der Parameter definiert die Art, wie in einem IP-Netzverbund der Zielpartner-Knoten identifiziert wird. Wertebereich: Nein, Erzwungen, Mehrere Standorte
Dediziertes Gateway: **Nein**	Der Partner-Knoten wird anhand der Ziel-Rufnummer identifiziert.
Dediziertes Gateway: **Erzwungen**	Es wird zwingend zu dem Gateway geroutet, das in der Spalte **GW Knoten-ID** durch seine Knoten-ID definiert ist.
Dediziertes Gateway: **Mehrere Standorte**	Anruferorientierte Bestimmung des Partner-Knotens: es wird zu dem Gateway geroutet, das dem jeweiligen Anrufer per Multigateway-Wizard oder in der Eingabemaske **Teilnehmer > Workpointclient Daten ändern > ID des Sekundärsystems** zugewiesen wurde. Für Anrufer ohne einen diesbezüglichen Eintrag wird zu dem Gateway geroutet, das in der Spalte **GW Knoten-ID** durch seine Knoten-ID definiert ist (default).
GW Knoten-ID	Angabe der Gateway-Knoten-ID für die Auswahl **Erzwungen** oder **Mehrere Standorte** des Parameters **Dediziertes Gateway**.

27.3.5.5 LCR > Wahlregel

Parameterbeschreibung der Registerkarte:

- **Wahlregel ändern**

Parameter	Beschreibung
	Durch die LCR-Wahlregeln können eingegebene Rufnummern zur Weiterverarbeitung in beliebige neue Ziffernfolgen umgewandelt werden. Durch Ziffernumwandlung wird der Zugang zu verschiedenen Netzanbietern ermöglicht. Die verwendete Wahlregel wird bestimmt durch den Eintrag in der Wegetabelle.
Regelname	Frei definierbarrer Name der Wahlregel, einige Wahlregeln sind vordefiniert Wertebereich: max. 16 Zeichen
Wahlregelformat	Programm für die zu wählenden Ziffern. Der einzelnen Programmschritte werden von links nach rechts abgearbeitet. Die Zeichen für den Programmcode stehen für folgende Funktionen:
A	Restliche Felder wiederholen (aussenden). "A" bewirkt, dass alle nachfolgenden Ziffernfelder gesendet werden. Bezugspunkt ist das letzte Feldtrennzeichen im Feld gewählte Ziffern im Wahlplan. Wird "A" ohne expliziten Bezug eingetragen, bezeichnet dies alle Ziffern nach dem Acces Code, d. h, "A" entspricht dann "E2A"
B	Wird für die Multi-Gateway-Vernetzung genutzt, wenn eine von extern angerufene Rufnummer vom TON (Type Of Number) "unknown" ist, um sie zum Multi-Gateway-Knoten zu routen. Damit diese Rufnummer eindeutig ist, wird sie entsprechend der TON im LCR auf national oder international erweitert. Dies ist erforderlich, wenn die Durchwahlnummern nicht eindeutig sind und ins nationale oder internationale Format konfiguriert werden müssen.

Parameter	Beschreibung
D (n)	Ziffernfolge wählen (1 bis 25 Ziffern). "D" darf in der Zeichenkette mehrmals vorkommen und an beliebigen Stellen stehen.
E (n)	Aussenden des Feldinhaltes (1 bis 10). "E" darf in der Zeichenkette mehrmals vorkommen und an beliebigen Stellen stehen. Die Reihenfolge von "E" in Abhängigkeit von (n) ist beliebig. Ein bestimmtes Feld darf mehrmals, auch aufeinanderfolgend, angesprochen werden. "E" darf mit Ausnahme von "E1" (Access Code) von beliebigen anderen Parametern eingeschlossen sein Bei schritthaltender Wahl (Gegensatz zur Blockwahl) darf das letzte Element in der Wahlregel nicht E(n) heißen, sondern E(n)A.
M (n)	Autorisierungscode (1 bis 16). Dieser Buchstabe darf nicht an der letzten Stelle stehen.
P (n)	Pause, "P" darf in der Zeichenkette mehrmals vorkommen und an beliebigen Stellen stehen.
S	Switch, Umschalten des Wahlverfahrens von IWV auf MFV (bei CONNECT, PROGRESS oder CALL PROC mit PI). "S" darf in der Zeichenkette nur einmal vorkommen und darf nicht an der letzten Stelle stehen. Nach "S" darf nicht mehr der Parameter "C" verwendet werden.
C	Carrier "C" darf in der Zeichenkette nur einmal vorkommen. Die nachfolgenden Zeichen werden ohne Wahlpause gesendet und für den Carrierzugang bei "Single Stage", "Two Stage", "DICS" und "PRI" verwendet.
U	Anwenden des Wahlverfahrens SUB-Adresse. "U" darf in der Zeichenkette nur einmal vorkommen und darf nicht an der letzten Stelle stehen. Nach "U" dürfen die Parameter "S", "P" "M" und "C" nicht mehr verwendet werden.
N (n) (Nur für USA!)	Netz-SFG-Gruppe (1 bis 5) oder Bandnummer (1).
L (Nur für USA!)	"L" darf nur am Ende der Zeichenkette vorkommen. "L" bewirkt, dass der Anruf als Notruf behandelt wird.
Verfahren des Netzanbieters	Auswahl des jeweiligen Netzanbieters
Unbekannt	Keine explizite Angabe über einen Netzanbieter.
Hauptnetzanbieter	Bei einer Belegung über den Hauptnetzanbieter erfolgt die einfache Wahl durch Blockwahl oder Wahl einzelner Ziffern in das öffentliche Netz.
MCL Single Stage	Bei MCL Single Stage wird mit einem Präfix der gewünschte Netzanbieter angewählt und anschließend die Rufnummer gewählt. Die Wahl erfolgt dabei bei ISDN im D-Kanal bzw. als normale Wahl bei HKZ.
MCL Two Stage	Bei MCL Two Stage wird mit einem Präfix der gewünschte Netzanbieter angewählt. Nach einer Synchronisationsphase wird zunächst ein ebenfalls konfigurierbarer Authorisierungscode und darauffolgend die Ziel-Rufnummer als DTMF-Zeichen gesendet Bei Synchronisation durch Zeit muss eine Pause von 2 bis 12 s programmiert werden.
Corporate Network	Ein Corporate Network ist direkt an OpenScape Business angeschlossen. Die LCR-Funktion bestimmt aus der vom Teilnehmer gewählten Nummer die entsprechende Richtung und routet das Gespräch entweder über das Leitungsbündel des öffentliches Amtes oder über das Leitungsbündel mit dem firmeneigenen Netz.

Parameter	Beschreibung
Dial In Control Server	Bei dieser Art LCR wird mit einem Präfix der gewünschte Netzanbieter über einen Dial-In Control Server (DICS) angewählt und dabei die Rufnummer und ein konfigurierbarer Authorisierungscode in der Subadresse übermittelt. Die Wahl erfolgt dabei im D-Kanal.
Primary Rate Interface (Primärmultiplexschnittstelle) (nur für USA)	Beim Primary Rate Interface erfolgt die Auswahl des Netzanbieters bzw. des Calling Service in der SETUP-Meldung über die Informationselemente Network Specific Facility, Operator System Access und Transit Network Selection.
Type	Type of Number [TON]; hier können pro Wahlregel folgende Nummerntypen der „Called Party Number“ über die Klappliste ausgewählt werden: Anlagenrufnummer, Ortsnetzkennzahl, Ländervorwahl. Als Default-Eintrag ist „Unbekannt“ vorgegeben. Der Type of Number wird nur bei E.164 gesetzt, bei einer Vernetzung steht der Parameter auf "unbekannt".

27.3.6 Sprachgateway

Unter **Sprachgateway** sind die Funktionen für die IP-Telefonie zusammengefasst.

27.3.6.1 Sprachgateway > SIP-Parameter

Parameterbeschreibung der Registerkarten:

- **SIP-Parameter ändern**

Parameter	Beschreibung
SIP Transport-Protokoll	
SIP über TCP	Abkürzung für „Transmission Control Protocol“. Ist neben IP das zentrale Protokoll im Internet. Es stellt einen verbindungsorientierten, zuverlässigen, Vollduplex-Dienst in Form eines Datenstroms zur Verfügung. Wird u.a. verwendet bei Vernetzung.
SIP über UDP	Abkürzung für „User Datagram Protocol“. Kann alternativ zu TCP verwendet werden, wenn keine Anforderungen an die Zuverlässigkeit gestellt werden. UDP garantiert weder die Zustellung der Pakete, noch ist eine bestimmte Reihenfolge des Eintreffens von Paketen gewährleistet. Wird u.a. verwendet bei Client-Protokollen über ITSP.
SIP über TLS	Abkürzung für „Transport Layer Security“. Wird verwendet für verschlüsselte Datenübertragungen.
SIP-Registrar	
Dauer der Registrierung (s)	Intervall (in Sekunden), in dem die Registrierung wiederholt wird. Der Wert des Intervalls sollte nicht zu hoch gesetzt sein, da mit der wiederholten Registrierung auch ein Verbindungsausfall erkannt wird und ggf. ein Ersatzweg (über ISDN oder einen alternativen Provider) belegt werden kann. Wertebereich, Standardwert: 10 - 86400, 120
RFC 3261 Timer-Werte	

Parameter	Beschreibung
Transaction Timeout (ms)	Gibt die Wartezeit (in Millisekunden) vor einer Neuübertragung der Invite-Antwort für den Zeitgeber D für die Spezifikation RFC 3261 an. Diese Einstellung ist für die Invite-Clienttransaktion relevant. Wertebereich, Standardwert: 2000 - 64000, 32000
SIP-Session-Timer	
RFC 4028 verwenden	RFC 4028 definiert eine Erweiterung des Session Initiation Protocols (SIP). Diese Erweiterung erlaubt einen periodischen Refresh von SIP-Sessions. Die User-Agents und die Proxies können durch den Refresh ermitteln, ob die SIP-Session noch aktiv ist.
Session-Expires (s)	Definiert die längste Dauer einer SIP-Session. Der empfohlene Wert ist „1800“. Dieser Wert sollte möglichst nicht unterschritten werden. Wertebereich, Standardwert: 90 - 65535, 1800
Minimal-SE (s)	Definiert die kürzeste Dauer einer SIP-Session, die erlaubt ist. Wertebereich, Standardwert: 90 - 65535, 90
Provider-Anrufe	
Maximal mögliche Anrufe über Provider	Anzahl der gleichzeitigen Gespräche über alle aktivierten Provider. Die maximale Anzahl ist von der Datenrate zum Internet und dem verwendeten Codec abhängig. Szenario: Pro aktivierten Provider wird eine Anzahl von Leitungen eingerichtet z.B. 2, das würde bei 4 aktivierten Providern 8 Leitungen ergeben. Ist aber die Bandbreite nur für 4 Gespräche vorhanden, dann verhindert dieser Parameter einen Aufbau eines 5. Gespräches und damit eine Störung der Payload.

27.3.6.2 Sprachgateway > Codec-Parameter

Parameterbeschreibung der Registerkarten:

- **Codec-Parameter ändern**

Parameter	Beschreibung
Codec	Die Parameter für die Codecs G.711 A-law, G.711 µ-law, G.729A und G.729AB können bearbeiten werden.
Codec: G.711 A-law	G.711 (A-law und µ-law): Sprachkodierung mit 56 oder 64 Kbit/s - sehr gute Sprachqualität. G.711 wird auch im Festnetzbereich (ISDN) eingesetzt. Das A-law-Verfahren ist ein primär in Europa verwendetes Digitalisierungsverfahren für analoge Audiosignale im Telekommunikationsbereich.
Codec: G.711 µ-law	G.711 (A-law und µ-law): Sprachkodierung mit 56 oder 64 Kbit/s - sehr gute Sprachqualität. G.711 wird auch im Festnetzbereich (ISDN) eingesetzt. In Nordamerika und Japan wird das ähnliche µ-law-Verfahren eingesetzt, das dem A-law ähnelt, jedoch nicht kompatibel ist. Zur Kommunikation, z. B. bei einem Telefongespräch zwischen Europa und USA, müssen die digitalen Daten durch entsprechende Konverter umgesetzt werden.
Codec: G.729A	Sprachkodierung mit 8 Kbit/s.
Codec: G.729AB	Sprachkodierung mit 8 Kbit/s. Auffüllen von Sprachpausen mit Komfortrauschen.

Parameter	Beschreibung
Priorität	Den Audio-Codecs können Prioritäten von 1 (hoch) bis 4 (niedrig) zugewiesen werden. Das Kommunikationssystem versucht automatisch, für jede Verbindung einen Audio-Codec mit einer möglichst hohen Priorität zu verwenden. Wird ein Audio-Codec mit geringer Sprachkomprimierung (guter Sprachqualität) verwendet, wird das Netz höher ausgelastet. Bei intensiver IP-Telefonie kann das bei einem durch Datentransfer bereits ausgelasteten Netz zu einer Verschlechterung der Sprachqualität führen.
Sprechpausenerkennung (VAD)	Aktivieren der Sprechpausenerkennung (VAD, Voice Activity Detection). Bei langen Sprechpausen kann somit die Last auf das Netz reduziert werden.
Rahmengröße	Für jeden Codec kann die Rahmengröße (Größe des IP-Pakets) von 10 bis zu 90 Millisekunden angegeben werden. Damit wird die Abtastrate festgelegt, mit der das Sprachsignal in IP-Pakete zerlegt wird. Ein höherer Wert (z. B. 90 ms) bedeutet einerseits ein besseres Verhältnis von Nutzdaten zum IP-Paket-Overhead, andererseits aber eine größere Verzögerung bei der Übertragung. Die einstellbaren Werte sind von den Codecs abhängig. Für Vernetzung von OpenScape Business mit OpenScape Voice über SIP-Q V2: Cordless IP und OpenScape Mobile Connect unterstützen nur eine Rahmengröße von 20 ms für den Codec G.711. Wenn es im Netzverbund eines dieser beiden Produkte gibt, muss hier die Rahmengröße auf 20 ms eingestellt werden. Wertebereich, Standardwert: 10 - max. 90, 20
Erweiterte DSP-Kanäle	
Nur G.711 verwenden	Nur die Protokolle G.711 A-law, G.711 µ-law werden verwendet. Bei G.711 werden weniger DSP-Ressourcen benötigt, dann sind mehr gleichzeitige Gespräche möglich.
T.38-Fax	
T.38-Fax	Legt fest, ob das T.38-Faxprotokoll zum Einsatz kommen soll.
FillBitRemoval verwenden	Legt fest, ob bei Verwendung des T.38-Faxprotokolls Füllbits beim Senden gelöscht und beim Empfangen wiederhergestellt werden sollen. Dadurch lässt sich Bandbreite sparen.
Max. UDP-Datagramm-Größe für T.38-Fax (Byte)	Maximale Größe eines T.38-UDP-Datagramms in Bytes. Wertebereich, Standardwert: 1 - 1472, 1472
Verwendete Fehlerkorrektur für T.38-Fax (UDP)	Legt fest, welche Methode zur Fehlerkorrektur eingesetzt werden soll. Wertebereich, Standardwert: t38UDPFEC, t38UDPRedundancy
Sonstiges	
ClearChannel	Ein ClearChannel ist ein offener Kanal, bei dem die Endpunkte für das Protokoll im Kanal verantwortlich sind. Der Parameter legt fest, ob die ClearChannel-Interface-Funktionalität aktiviert sein soll oder nicht.
Rahmengröße	In diesem Feld können Sie die Sampling-Rate bestimmen. Möglich sind 10, 20, 30, 40, 50 und 60 Millisekunden (ms). Wertebereich, Standardwert: 10 - 60, 20
RFC2833 RFC2833 legt fest, wie die Tonsignale übermittelt werden.	
Übertragung von Fax/Modem Tönen nach RFC2833	Übertragung outband (über die SIP-Signalisierung), empfohlene Betriebsweise um Töne sicher zu übertragen

Parameter	Beschreibung
Übertragung von DTMF Tönen nach RFC2833	Übertragung outband (über die SIP-Signalisierung), empfohlene Betriebsweise um Töne sicher zu übertragen
Payload Type für RFC2833	Anpassung ggf. abhängig vom Kommunikationspartner erforderlich Wertebereich, Standardwert: 96 - 126, 98
Redundante Übertragung der RFC2833 Töne nach RFC2198	Dient zur Erhöhung der Übertragungssicherheit

27.3.6.3 Sprachgateway > Ziel-Codec-Parameter

Für bestimmte Kommunikationspartner können Prioritäten für die Verwendung der Audio-Codecs definiert werden.

Parameterbeschreibung der Registerkarten:

- **Ziel-Codec-Parameter hinzufügen**

Parameter	Beschreibung
Codec: G.711 A-law	G.711 (A-law und µ-law): Sprachkodierung mit 56 oder 64 Kbit/s - sehr gute Sprachqualität. G.711 wird auch im Festnetzbereich (ISDN) eingesetzt. Das A-law-Verfahren ist ein primär in Europa verwendetes Digitalisierungsverfahren für analoge Audiosignale im Telekommunikationsbereich.
Codec: G.711 µ-law	G.711 (A-law und µ-law): Sprachkodierung mit 56 oder 64 Kbit/s - sehr gute Sprachqualität. G.711 wird auch im Festnetzbereich (ISDN) eingesetzt. In Nordamerika und Japan wird das ähnliche µ-law-Verfahren eingesetzt, das dem A-law ähnelt, jedoch nicht kompatibel ist. Zur Kommunikation, z. B. bei einem Telefongespräch zwischen Europa und USA, müssen die digitalen Daten durch entsprechende Konverter umgesetzt werden.
Codec: G.729A	Sprachkodierung mit 8 Kbit/s.
Codec: G.729AB	Sprachkodierung mit 8 Kbit/s. Auffüllen von Sprachpausen mit Komfortrauschen.
Priorität	Den Audio-Codecs können Prioritäten von 1 (hoch) bis 4 (niedrig) zugewiesen werden. Das Kommunikationssystem versucht automatisch, für jede Verbindung einen Audio-Codec mit einer möglichst hohen Priorität zu verwenden. Wird ein Audio-Codec mit geringer Sprachkomprimierung (guter Sprachqualität) verwendet, wird das Netz höher ausgelastet. Bei intensiver IP-Telefonie kann das bei einem durch Datentransfer bereits ausgelasteten Netz zu einer Verschlechterung der Sprachqualität führen.
Ziel	
Ziel-Adress-Typ	Anzeige des Typs des Ziels, dem die eingestellten Prioritäten der Audio-Codecs zugeordnet werden sollen.
IP-Adresse	IP-Adresse des Ziels, für das die eingestellten Prioritäten der Audio-Codecs gelten sollen (z.B. vernetzter Knoten, SIP Server)

27.3.6.4 Sprachgateway > Internet-Telefonie Service Provider

Parameterbeschreibung der Registerkarten:

- **Internet Telefonie Service Provider hinzufügen**

- **Internet Telefonie Service Provider ändern**
- **Internet Telefonie Service Provider löschen**

Parameter	Beschreibung
Template verwenden	Auswahl einer leeren (default) oder einer für einen bestimmten Service Provider vordefinierten Musterkonfiguration. Diese kann an die eigenen Belange angepasst und als neuer ITSP abgespeichert werden.
Provider-Name	Gewünschter Name des ITSP. Unter diesem Namne wird der konfigurierte ITSP in der Liste der ITSP aufgeführt.
Provider aktivieren	Der ITSP wird aktiviert.
Providerbezeichner im System	Zuordnung einer eindeutigen Bezeichnung im System. Es können maximal 4 Provider gleichzeitig aktiv sein. Wertebereich: Provider 1 - 4
Gateway Domain Name	Gateway-Domänennamen des ITSP. Häufig nicht identisch mit dem Web Domänen-Namen.
Provider-Registrar	
Provider Registrar verwenden	Auszuwählen, wenn der ITSP mit Registrierung arbeitet.
IP Adresse/Host-Name	Domänenname oder IP-Adresse des Registrar-Servers (z. B. sip-voice.de).
Port	Portnummer des Registrar-Servers z. B. 5060. Port 0 eintragen, wenn der ITSP mit mehreren Servern und DNSSRV arbeitet.
Reregistration-interval am Provider (s)	Intervall (in Sekunden), in dem die Registrierung am ITSP wiederholt wird. Der Wert des Intervalls darf nicht 0 sein und sollte nicht zu hoch gesetzt sein, da mit der wiederholten Registrierung am ITSP auch ein Verbindungsausfall erkannt wird und ggf. ein Ersatzweg (über ISDN oder einen alternativen Provider) belegt werden kann. Standardwert: 120 Sekunden.
Provider-Proxy	
IP Adresse/Host-Name	Domänenname oder IP-Adresse des Proxy-Servers (z. B. sip-voice.de). Der Eintrag ist zwingend notwendig und ist in der Regel identisch zum Provider-Registrar-Eintrag.
Port	Portnummer des Proxy-Servers (z. B. 5060). Ist in der Regel identisch zur Provider-Registrar-Portnummer. Port 0 eintragen, wenn der ITSP mit mehreren Servern und DNSSRV arbeitet.
Provider-Outbound-Proxy	
Provider Outbound-Proxy verwenden	Wird nur gesetzt, wenn der ITSP einen Outbound-Proxy verwendet, der sich von dem Provider Proxy unterscheidet.
IP Adresse/Host-Name	Domänenname oder IP-Adresse des Outbound-Proxy.
Port	Portnummer des Outbound-Proxy. Port 0 eintragen, wenn der ITSP mit mehreren Servern und DNSSRV arbeitet.
Provider-Inbound-Proxy	
Provider Inbound-Proxy verwenden	Wird nur gesetzt, wenn der ITSP Anfragen wahlweise von einem zweiten Servern sendet.
IP Adresse/Host-Name	Domänenname oder IP-Adresse des zweiten ITSP-Servers
Port	Portnummer des zweiten ITSP Servers. Port 0 eintragen, wenn der ITSP mit mehreren Servern und DNSSRV arbeitet.

Parameter	Beschreibung
Provider-STUN	
STUN verwenden	Wird nur gesetzt, wenn der ITSP einen STUN-Server verwendet. Als STUN -Modus für alle ITSP gilt die systemweite Einstellung unter STUN Konfiguration.
IP Adresse/Host-Name	STUN-IP-Adresse, wenn der ITSP einen STUN-Server verwendet.
Port	STUN-Port-Nummer, wenn der ITSP einen STUN-Server verwendet.
Extended SIP Provider Data	
Erweiterte SIP Provider Daten anzeigen	Eine Anpassung dieser Daten ist üblicherweise nur im Rahmen von Tests mit neuen ITSPs notwendig. Details sind im VoIP Provider Data Collection Document auf wiki.unify.com beschrieben.
Schaltflächen	
Restart ITSP	Bewirkt eine Neuregistrierung beim ITSP (nur bei aktiviertem ITSP möglich).

Parameterbeschreibung der Registerkarten:

- **STUN-Konfiguration ändern**

Parameter	Beschreibung
STUN-Modus	Diese Einstellung gilt global für alle ITSPs, sofern STUN für diese aktiv ist.Ob STUN benötigt wird ist abhängig von der ITSP-Infrastruktur und dem verwendeten Internet-Router. STUN wird nicht benötigt, wenn der ITSP NAT-Traversal im eigenen Netz auflöst. STUN sorgt dafür, dass in SIP-Meldungen die öffentlich erreichbare IP-Adresse anstelle der internen IP Adresse verwendet wird.
STUN-Modus: Immer	STUN ist immer aktiv.
STUN-Modus: Automatisch	Es wird automatisch eine Überprüfung des NAT-Typs des Routers zum Internet vorgenommen. Wenn STUN benötigt wird, wird STUN eingeschaltet. Wenn kein STUN benötigt wird oder möglich ist, wird STUN ausgeschaltet. Dies ist die empfohlene Standardeinstellung.
STUN-Modus: statische IP verwenden	Wenn der ITSP eine statische IP-Autentifizierung verlangt ist eine statische IP-Adresse (öffentliche IP-Adresse) im DSL-Modem oder Internet-Router notwendig. Die verwendete statische IP-Adresse und Port müssen zusätzlich angegeben werden.
STUN-Modus: statische IP verwenden, Öffentliche IP-Adresse	Statische IP-Adresse des DSL-Modems oder des Internet-Routers.
STUN-Modus: statische IP verwenden, Öffentlicher SIP-Port	Port des DSL-Modems oder des Internet-Routers.
STUN-Modus: Router behält Port bei	Falls keiner der oben genannten STUN-Modi funktioniert, sollte dieser Modus ausprobiert werden. Einige Modems und Internet-Router ändern den RTP-Port nicht für NAT und benötigen diesen Modus für einen korrekten Betrieb.
Entdeckter NAT-Typ	Wenn ein ITSP aktiv ist, wird hier der NAT Typ angezeigt
Default STUN Server	
IP-Adresse / Hostname	IP-Adresse oder Hostnamen des STUN-Servers (z. B. `stun.serviceprovider.com`). Dieser STUN-Server wird für SIP@Home verwendet, wenn kein ITSP verwendet wird oder der genutzte ITSP kein STUN-Server anbietet.
Port	Port des STUN-Servers (z. B. `3478`)

Parameterbeschreibung der Registerkarten:

- **NAT-Typ entdecken**

Parameter	Beschreibung
Autom. Aktivierung	Aktiviert die automatische NAT-Typ-Entdeckung.
NAT-Typ-Entdeckung starten	Startet die NAT-Typ-Entdeckung manuell.

Parameterbeschreibung der Registerkarten:

- **Internet-Telefonie-Teilnehmer hinzufügen**
- **Internet-Telefonie-Teilnehmer ändern**
- **Internet-Telefonie-Teilnehmer löschen**

Parameter	Beschreibung
Internet-Telefonie-Teilnehmer	Zugangsdaten des Accounts, den der ITSP zugewiesen hat. Je nach ITSP werden hierfür unterschiedliche Bezeichnungen verwendet, wie z. B. SIP-User, SIP-Nutzer, SIP-ID. Evtl. ist hier auch die ITSP-Kundennummer einzutragen. Wird eine statische IP Authentifizierung verwendet, so ist hier die Anlagenrufnummer ienzutragen.
Autorisierungsname	Autorisierungsname, den der ITSP zugewiesen hat. Oft identisch mit Internet-Telefonie-Teilnehmer.
Kennwort	Kennwort, das der ITSP zugewiesen hat. Je nach ITSP werden hierfür unterschiedliche Bezeichnungen verwendet, wie z. B. SIP-Passwort oder SIP-Kennwort.
Kennwort wiederholen	Kennwort, das der ITSP zugewiesen hat. Je nach ITSP werden hierfür unterschiedliche Bezeichnungen verwendet, wie z. B. SIP-Passwort oder SIP-Kennwort.

Parameterbeschreibung der Registerkarten:

- **MSN Zugang hinzufügen**
- **MSN Zugang ändern**
- **MSN Zugang löschen**
- **Alle MSN-Einträge löschen**

Parameter	Beschreibung
Internet-Telefonie-Rufnummer / **Internet-Telefonie-Teilnehmer-rufnummer** / **DSL-Telefonie-Teilnehmerrufnummer**	Vom ITSP zugewiesene (Einzel-)Rufnummer.
Durchwahl / **interne Rufnummer**	Zugeordnete interne Rufnummer.
Default-Eintrag	Die Aktivierung als Default-Eintrag ermöglicht Teilnehmern, die keine eigene Internet-Telefonie-Rufnummer haben, Gespräche über diese Nummer zu führen. Die Option kann nur für eine MSN ausgewählt werden.
Internet-Telefonie-Teilnehmer / **DSL-Telefonie-Teilnehmer**	Anzeige des Internet-Telefonie-Teilnehmers.

Parameterbeschreibung der Registerkarten:

- **Durchwahl-Bereich hinzufügen**
- **Durchwahl-Bereich ändern**
- **Durchwahl-Bereich löschen**

Parameter	Beschreibung
Anlagenrufnummer	Vom ITSP zugewiesene Kopfrufnummer (ohne die Durchwahlnummer)
Durchwahlband von … bis	Bereich der vom ITSP zugewiesenen Durchwahlnummern
Beginn interner Rufnummern-Bereich	Erste interne Rufnummer, ab der eine automatische Zuordung der Rufnummern gewünscht wird.
Durchwahlband automatisch den Teilnehmern zuordnen	Wenn ausgewählt, werden die Durchwahlnummern automatisch aufsteigend den internen Rufnummern zugeordnet und es werden entsprechende MSN-Einträge erzeugt.

27.3.6.5 Sprachgateway > Networking > Knoten

Parameterbeschreibung der Registerkarten:

- **Networking-Knoten hinzufügen**
- **Networking-Knoten ändern**
- **Networking-Knoten löschen**

Parameter	Beschreibung
Knoten ID	Nur für manuelle Konfiguration ohne Wizard z. B. bei offener Nummerierung: Eingabe einer Knotennummer, die im Netzverbund eindeutig ist.
IP-Adresse	Nur für manuelle Konfiguration ohne Wizard z. B. bei offener Nummerierung: IP-Adresse des Knotens
Knotenüberwachung	Die Auswahl der Knotenüberwachung bewirkt eine periodische Überprüfung der Kommunikation mit dem Knoten. Voraussetzung ist, dass die Knotenüberwachung auch im anderen Knoten aktiviert ist.
Verschlüsselungseinstellung des Knoten	Durch die Auswahl von "sicher" wird die Verschlüsselung für die Sprachkommunikation mit dem Knoten aktiviert. Hierzu muss zusätzlich im System "Signaling und Payload Encryption" eingerichtet werden. Wertebereich: traditionell, sicher

27.3.6.6 Sprachgateway > Networking > Routing

Parameterbeschreibung der Registerkarten:

- **Rufnummer hinzufügen**
- **Alle Rufnummern löschen**

Parameter	Beschreibung
Knoten ID	Auswahl der Knotennummer
Rufnummer	Nur für manuelle Konfiguration ohne Wizard z. B. bei offener Nummerierung: Angabe der Kennzahl über die der Knoten erreichbar ist.

27.3.6.7 Sprachgateway > SIPQ-Verbindung

Über die SIPQ-Verbindung werden die Parameter für zwei mögliche externe SIP-Richtungen definiert. Über diese können beliebige externe SIP-Server wie z. B. OpenScape 4000/HiPath 4000, OpenScape Voice, oder auch native SIP Server Trunks angeschaltet werden. Entsprechende Beispiele sind in den vorhandenen Templates eingepflegt.

Parameterbeschreibung der Registerkarten:

- **SIPQ-Verbindung hinzufügen**
- **SIPQ-Verbindung ändern**
- **SIPQ-Verbindung löschen**

Parameter	Beschreibung
Template verwenden	Template, das als Basis verwendet werden soll.
Name	Name des externen SIP-Servers (Template-Name).
Trunk aktivieren	Die Verbindung zum externen SIP-Server ist aktiviert. Standardwert: deaktiviert
Trunk-ID im System	Auswahl zwischen zwei externen SIP-Verbindungen. Wenn vorhanden, ist eine der beiden SIP-Verbindungen immer mit der UC Booster Card oder dem UC Booster Server belegt.
Name der Remote-Domäne	Hostname oder IP-Adresse der externen SIP-Servers. Der Wert ist in der Regel identisch mit dem Wert bei **IP Adresse/Host-Name**.
SIP-Server	
IP Adresse/Host-Name	Hostname oder IP-Adresse des externen SIP-Servers.
Port	SIP-Port des externen SIP-Servers (z. B. 5060 oder 5061). Wertebereich: 0 oder 1024-65535
Sicherer Transport	Bei Anschaltung an OpenScape 4000/HiPath 4000 oder OpenScape Voice kann die verschlüsselte SIP-Signalisierung aktiviert werden (Signalling and Payload Encryption feature). Standardwert: deaktiviert
SIP-Registrar	
Provider Registrar verwenden	Externer SIP-Server erfordert eine Registrierung. Standardwert: deaktiviert
IP Adresse/Host-Name	Hostname oder IP-Adresse des Registrar-Servers.
Port	Portnummer des Registrar-Servers (z. B. 5060). Wertebereich: 0 oder 1024-65535
Reregistrierungsintervall (s)	Intervall (in Sekunden), in dem die Registrierung wiederholt wird. Wertebereich: Minimaler Wert: 30, Maximaler Wert: 86400, Beispiel-Werte: 120 oder 240
Outbound Proxy/Inbound Proxy	

Parameter	Beschreibung
Provider Outbound/Inbound Proxy verwenden	Aktivierung des Outbound Proxy: Bestimmte Redundanz-Szenarien (z. B. mit OpenScape Branch Proxy) erfordern die Abwicklung der SIP-Signalisierung über einen Outbound Proxy. Aktivierung des Inbound Proxy: In bestimmeten Redundanz-Szenarien (z. B. mit OpenScape Voice) erfolgt die ankommende Signalisierung von einem separaten SIP-Server (Inbound proxy). Standardwerte: jeweils deaktiviert
IP Adresse/Host-Name	Hostname oder IP-Adresse des Outbound bzw. Inbound Proxy.
Port	Portnummer des Outbound bzw. Inbound Proxy (z.B. 5060). Wertebereiche: 0 oder 1024-65535

Parameterbeschreibung der Registerkarten:

- **SIPQ-Verbindungsteilnehmer hinzufügen**
- **SIPQ-Verbindungsteilnehmer ändern**
- **SIPQ-Verbindungsteilnehmer löschen**

Parameter	Beschreibung
Benutzer-ID	Eingabe der Benutzer-ID für den Zugang zum SIP-Server.
Autorisierungsname / **Realm**	Eingabe des Autorisierungsnamens oder der Realm für den Zugang zum SIP-Server.
Kennwort	Eingabe des Kennworts für den Zugang zum SIP-Server.
Kennwort wiederholen	Wiederholung des Kennworts für den Zugang zum SIP-Server.

27.3.7 Teilnehmer

Unter **Teilnehmer** sind die Funktionen für alle Teilnehmer zusammengefasst. Dazu gehören z. B. Name und Rufnummer der Teilnehmer, aber auch die Tastenprogrammierung.

27.3.7.1 Teilnehmer > Teilnehmer > UP0 Teilnehmer

Parameterbeschreibung der Registerkarten:

- **Teilnehmer ändern**

Parameter	Beschreibung
Rufnr	Interne Rufnummer des Teilnehmers.
DuWa	Durchwahlnummer des Teilnehmers.
Name	Frei wählbarer Name des Teilnehmers. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen

Parameter	Beschreibung
Clip/Lin	Ziffernfolge, die beim einem gehenden externen Anruf beim Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird (z.B. für Notrufdienst E911 USA) Wertebereich: max. 16 Ziffern
Aktiv	Zeigt an, ob der Teilnehmer betriebsbereit ist.
Endgeräte Typ	Anzeige des dem Teilnehmer zugeordneten Endgeräts.
Fax Rufnr	Falls eine Faxbox eingerichtet ist (z. B. mit den UC Clients myPortal for Desktop oder myPortal for Outlook), hier die Fax-Rufnummer eintragen, unter der der Teilnehmer von intern Faxnachrichten empfangen kann.
Fax DuWa	Falls eine Faxbox eingerichtet ist (z. B. mit den UC Clients myPortal for Desktop oder myPortal for Outlook), hier die Fax-Rufnummer eintragen, unter der der Teilnehmer von extern Faxnachrichten empfangen kann.
Zugang	Anzeige der physikalischen Schnittstelle, an der das Endgerät angeschlossen ist.
Suche	Sie können sich auch ausgewählte Teilnehmer anzeigen lassen, indem Sie in die **Suche**-Felder den Suchbegriff eingeben und mit der Return-Taste bestätigen. Die zu dem Suchbegriff passenden Teilnehmer werden angezeigt. Sind alle **Suche**-Felder leer und wird die Return-Taste gedrückt, werden wieder alle Teilnehmer aufgelistet.
Einträge pro Seite	Auswahl, ob 10, 25, 50 oder 100 Einträge pro Seite angezeigt werden sollen.
Schaltflächen	
Blauer Pfeil in Spalte **Rufnr**	Ruft die Seite mit den Registerkarten **Teilnehmer-Parameter ändern**, **Teilnehmer-Flags ändern**, **Workpointclient Daten ändern** und **Gruppen/RWS ändern** auf.
>	Springt eine Seite weiter.
<	Springt eine Seite zurück.
>|	Springt zum Ende der Liste.
|<	Springt zum Anfang der Liste.

Parameterbeschreibung der Registerkarten:

- **UP0 Master/Slave**
  Diese Registerkarte gibt es nur bei OpenScape Business X8, da bei diesem System die Slave-Ports dynamisch verwaltet werden. Bei OpenScape Business X1/X3/X5 sind die Slave-Ports fest zugeordnet.

Parameter	Beschreibung
Rufnr	Interne Rufnummer des Teilnehmers.
DuWa	Durchwahlnummer des Teilnehmers.
Name	Frei wählbarer Name des Teilnehmers. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Zugang	Anzeige der physikalischen Schnittstelle, an der das Endgerät angeschlossen ist.

Parameter	Beschreibung
Slave hinzufügen	Ist dieses Kontrollkästchen aktiviert, wird dem ausgewählten Master-Port vorbereitend ein Slave-Port zugeordnet. Nach Speichern der Auswahl mit **Übernehmen** können vorab Rufnummer, Durchwahl und Name des Slave-Systemtelefons konfiguriert werden. Wird anschließend an dem Slave-Adapter des Master-Systemtelefons das Slave-Systemtelefon angeschlossen, wird es dem zuvor ausgewählten Slave-Port zugewiesen. Wird das Slave-Systemtelefon ohne vordefiniertem Slave-Port angeschlossen, wird automatisch der nächste freie Port (ab Port 384) belegt.
Slave löschen	Ist dieses Kontrollkästchen aktiviert, wird die Vorkonfiguration des Slave-Systemtelefons gelöscht. Ist ein Slave-Systemtelefon an dem Slave-Adapter des Master-Systemtelefons angeschlossen, ist das Kontrollkästchen ausgegraut. Die Vorkonfiguration kann nicht gelöscht werden.
Suche	Sie können sich auch ausgewählte Teilnehmer anzeigen lassen, indem Sie in die **Suche**-Felder den Suchbegriff eingeben und mit der Return-Taste bestätigen. Die zu dem Suchbegriff passenden Teilnehmer werden angezeigt. Sind alle **Suche**-Felder leer und wird die Return-Taste gedrückt, werden wieder alle Teilnehmer aufgelistet.
Einträge pro Seite	Auswahl, ob 10, 25, 50 oder 100 Einträge pro Seite angezeigt werden sollen.
Schaltflächen	
>	Springt eine Seite weiter.
<	Springt eine Seite zurück.
>|	Springt zum Ende der Liste.
|<	Springt zum Anfang der Liste.

Parameterbeschreibung der Registerkarten:

- **Endgeräte Info**

Parameter	Beschreibung
Rufnr	Interne Rufnummer des Teilnehmers.
Name	Name des Teilnehmers.
Endgeräte Typ	Anzeige des dem Teilnehmer zugeordneten Endgerätes.
Aktuelle SW-Version	Software-Version des zugeordneten Endgerätes (sofern verfügbar).
HW-Version	Hardware-Version des zugeordneten Endgerätes (sofern verfügbar).
Einträge pro Seite	Auswahl, ob 10, 25, 50 oder 100 Einträge pro Seite angezeigt werden sollen.
Schaltflächen	
>	Springt eine Seite weiter.
<	Springt eine Seite zurück.
>|	Springt zum Ende der Liste.
|<	Springt zum Anfang der Liste.

27.3.7.2 Teilnehmer > Teilnehmer > IP Clients

Parameterbeschreibung der Registerkarten:

- **Teilnehmer ändern**

Parameter	Beschreibung
Rufnr	Interne Rufnummer des Teilnehmers.
DuWa	Durchwahlnummer des Teilnehmers.
Name	Frei wählbarer Name des Teilnehmers. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Typ	Typ des Teilnehmers.
Typ: **Frei**	Dieser Rufnummer ist (noch) kein Teilnehmer zugeordnet.
Typ: **System Client**	Ein System-Client ist ein IP-Teilnehmer, der über CorNet-IP alle Leistungsmerkmale des Kommunikationssystems nutzen kann (früher HFA System-Client)
Typ: **RAS User**	Einem RAS-User (Remote Access Service User) wird über den ISDN-Anschluss der Zugang zum IP-Netz gewährt. Dadurch kann das Kommunikationssystem ferngewartet und lizenziert werden.
Typ: **SIP Client**	Ein SIP-Client ist ein IP-Teilnehmer, der das Protokoll SIP nutzt. Er kann über SIP nur einen eingeschränkten Leistungsumfang des Kommunikationssystems nutzen.
Typ: **Deskshare User**	Ein Deskshare User ist ein IP-Teilnehmer, der sich auf einem anderen IP-Systemtelefon anmelden kann (Mobile Login) und dieses Telefon wie sein eigenes Telefon nutzen kann (inkl. Rufnummer).
Clip/Lin	Ziffernfolge, die beim einem gehenden externen Anruf beim Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird (z.B. für Notrufdienst E911 USA)
Aktiv	Zeigt an, ob der Teilnehmer betriebsbereit ist.
Fax Rufnr	Falls eine Faxbox eingerichtet ist (z. B. mit den UC Clients myPortal for Desktop oder myPortal for Outlook), hier die Fax-Rufnummer eintragen, unter der der Teilnehmer von intern Faxnachrichten empfangen kann.
Fax DuWa	Falls eine Faxbox eingerichtet ist (z. B. mit den UC Clients myPortal for Desktop oder myPortal for Outlook), hier die Fax-Rufnummer eintragen, unter der der Teilnehmer von extern Faxnachrichten empfangen kann.
Suche	Sie können sich auch ausgewählte Teilnehmer anzeigen lassen, indem Sie in die **Suche**-Felder den Suchbegriff eingeben und mit der Return-Taste bestätigen. Die zu dem Suchbegriff passenden Teilnehmer werden angezeigt. Sind alle **Suche**-Felder leer und wird die Return-Taste gedrückt, werden wieder alle Teilnehmer aufgelistet.
Einträge pro Seite	Auswahl, ob 10, 25, 50 oder 100 Einträge pro Seite angezeigt werden sollen.
Schaltflächen	
Blauer Pfeil in Spalte **Rufnr**	Ruft die Seite mit den Registerkarten **Teilnehmer-Parameter ändern**, **Teilnehmer-Flags ändern**, **Workpointclient Daten ändern** und **Gruppen/RWS ändern** auf.
>	Springt eine Seite weiter.

Parameter	Beschreibung
<	Springt eine Seite zurück.
>|	Springt zum Ende der Liste.
|<	Springt zum Anfang der Liste.

Parameterbeschreibung der Registerkarten:

- **Endgeräte Info**

Parameter	Beschreibung
Rufnr	Interne Rufnummer des Teilnehmers.
Name	Name des Teilnehmers.
Endgeräte Typ	Anzeige des dem Teilnehmer zugeordneten Endgerätes.
IP Adresse	IP-Adresse des zugeordneten Endgerätes; direkter Link zum WBM des IP-Telefons
MAC Adresse	MAC-Adresse des zugeordneten Endgerätes
Aktuelle SW Version	Software-Version des zugeordneten Endgerätes (sofern verfügbar).
HW Version	Hardware-Version des zugeordneten Endgerätes (sofern verfügbar).
Einträge pro Seite	Auswahl, ob 10, 25, 50 oder 100 Einträge pro Seite angezeigt werden sollen.
Schaltflächen	
>	Springt eine Seite weiter.
<	Springt eine Seite zurück.
>|	Springt zum Ende der Liste.
|<	Springt zum Anfang der Liste.

27.3.7.3 Teilnehmer > Teilnehmer > Analoge Teilnehmer

Parameterbeschreibung der Registerkarten:

- **Teilnehmer ändern**

Parameter	Beschreibung
Rufnr	Interne Rufnummer des Teilnehmers.
DuWa	Durchwahlnummer des Teilnehmers.
Name	Frei wählbarer Name des Teilnehmers. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Clip/Lin	Ziffernfolge, die beim einem gehenden externen Anruf beim Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird (z.B. für Notrufdienst E911 USA) Wertebereich: max. 16 Ziffern
Aktiv	Zeigt an, ob der Teilnehmer betriebsbereit ist.
Endgeräte Typ	Anzeige des dem Teilnehmer zugeordneten Endgeräts.

Parameter	Beschreibung
Fax Rufnr	Falls eine Faxbox eingerichtet ist (z. B. mit den UC Clients myPortal for Desktop oder myPortal for Outlook), hier die Fax-Rufnummer eintragen, unter der der Teilnehmer von intern Faxnachrichten empfangen kann.
Fax DuWa	Falls eine Faxbox eingerichtet ist (z. B. mit den UC Clients myPortal for Desktop oder myPortal for Outlook), hier die Fax-Rufnummer eintragen, unter der der Teilnehmer von extern Faxnachrichten empfangen kann.
Access	Anzeige der physikalischen Schnittstelle, an der das Endgerät angeschlossen ist.
Suche	Sie können sich auch ausgewählte Teilnehmer anzeigen lassen, indem Sie in die **Suche**-Felder den Suchbegriff eingeben und mit der Return-Taste bestätigen. Die zu dem Suchbegriff passenden Teilnehmer werden angezeigt. Sind alle **Suche**-Felder leer und wird die Return-Taste gedrückt, werden wieder alle Teilnehmer aufgelistet.
Einträge pro Seite	Auswahl, ob 10, 25, 50 oder 100 Einträge pro Seite angezeigt werden sollen.
Schaltflächen	
Blauer Pfeil in Spalte **Rufnr**	Ruft die Seite mit den Registerkarten **Teilnehmer-Parameter ändern**, **Teilnehmer-Flags ändern**, **Workpointclient Daten ändern** und **Gruppen/RWS ändern** auf.
>	Springt eine Seite weiter.
<	Springt eine Seite zurück.
>|	Springt zum Ende der Liste.
|<	Springt zum Anfang der Liste.

27.3.7.4 Teilnehmer > Teilnehmer > ISDN Teilnehmer

Parameterbeschreibung der Registerkarten:

- **Teilnehmer ändern**

Parameter	Beschreibung
Rufnr	Interne Rufnummer des Teilnehmers.
DuWa	Durchwahlnummer des Teilnehmers.
Name	Frei wählbarer Name des Teilnehmers. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Clip/Lin	Ziffernfolge, die beim einem gehenden externen Anruf beim Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird (z.B. für Notrufdienst E911 USA) Wertebereich: max. 16 Ziffern
Aktiv	Zeigt an, ob der Teilnehmer betriebsbereit ist.
Endgeräte Typ	Anzeige des dem Teilnehmer zugeordneten Endgeräts.
Fax Rufnr	Falls eine Faxbox eingerichtet ist (z. B. mit den UC Clients myPortal for Desktop oder myPortal for Outlook), hier die Fax-Rufnummer eintragen, unter der der Teilnehmer von intern Faxnachrichten empfangen kann.

Parameter	Beschreibung
Fax DuWa	Falls eine Faxbox eingerichtet ist (z. B. mit den UC Clients myPortal for Desktop oder myPortal for Outlook), hier die Fax-Rufnummer eintragen, unter der der Teilnehmer von extern Faxnachrichten empfangen kann.
Access	Anzeige der physikalischen Schnittstelle, an der das Endgerät angeschlossen ist.
Suche	Sie können sich auch ausgewählte Teilnehmer anzeigen lassen, indem Sie in die **Suche**-Felder den Suchbegriff eingeben und mit der Return-Taste bestätigen. Die zu dem Suchbegriff passenden Teilnehmer werden angezeigt. Sind alle **Suche**-Felder leer und wird die Return-Taste gedrückt, werden wieder alle Teilnehmer aufgelistet.
Einträge pro Seite	Auswahl, ob 10, 25, 50 oder 100 Einträge pro Seite angezeigt werden sollen.
Schaltflächen	
Blauer Pfeil in Spalte **Rufnr**	Ruft die Seite mit den Registerkarten **Teilnehmer-Parameter ändern**, **Teilnehmer-Flags ändern**, **Workpointclient Daten ändern** und **Gruppen/RWS ändern** auf.
>	Springt eine Seite weiter.
<	Springt eine Seite zurück.
>|	Springt zum Ende der Liste.
|<	Springt zum Anfang der Liste.

27.3.7.5 Teilnehmer > Teilnehmer > DECT-Teilnehmer > Basestations

Parameterbeschreibung der Registerkarten:

- **Teilnehmer ändern**

Parameter	Beschreibung
Rufnr	Interne Rufnummer des Teilnehmers.
DuWa	Durchwahlnummer des Teilnehmers.
Name	Frei wählbarer Name des Teilnehmers. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Clip/Lin	Ziffernfolge, die beim einem gehenden externen Anruf beim Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird (z.B. für Notrufdienst E911 USA) Wertebereich: max. 16 Ziffern
Aktiv	Zeigt an, ob der Teilnehmer betriebsbereit ist.
Endgeräte Typ	Anzeige des dem Teilnehmer zugeordneten Endgeräts. Basisstationen werden als S0-Teilnehmer angezeigt.
Access	Anzeige der physikalischen Schnittstelle, an der das Endgerät angeschlossen ist.
Parameter	Standardansicht für alle Teilnehmer, Einstellungen nicht verändern
Suche	Sie können sich auch ausgewählte Teilnehmer anzeigen lassen, indem Sie in die **Suche**-Felder den Suchbegriff eingeben und mit der Return-Taste bestätigen. Die zu dem Suchbegriff passenden Teilnehmer werden angezeigt. Sind alle **Suche**-Felder leer und wird die Return-Taste gedrückt, werden wieder alle Teilnehmer aufgelistet.
Einträge pro Seite	Auswahl, ob 10, 25, 50 oder 100 Einträge pro Seite angezeigt werden sollen.

Parameter	Beschreibung
Schaltflächen	
Blauer Pfeil in Spalte **Rufnr**	Ruft die Seite mit den Registerkarten **Teilnehmer-Parameter ändern**, **Teilnehmer-Flags ändern**, **Workpointclient Daten ändern** und **Gruppen/RWS ändern** auf.
>	Springt eine Seite weiter.
<	Springt eine Seite zurück.
>|	Springt zum Ende der Liste.
|<	Springt zum Anfang der Liste.

27.3.7.6 Teilnehmer > Teilnehmer > DECT-Teilnehmer > DECT Teilnehmer

Parameterbeschreibung der Registerkarten:

- **Teilnehmer ändern**

Parameter	Beschreibung
Rufnr	Interne Rufnummer des Teilnehmers.
DuWa	Durchwahlnummer des Teilnehmers.
Name	Frei wählbarer Name des Teilnehmers. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Clip/Lin	Ziffernfolge, die beim einem gehenden externen Anruf beim Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird (z.B. für Notrufdienst E911 USA) Wertebereich: max. 16 Ziffern
Aktiv	Zeigt an, ob der Teilnehmer betriebsbereit ist.
Endgeräte Typ	Anzeige des dem Teilnehmer zugeordneten Endgeräts. DECT-Teilnehmer werden als Comfort-PP angezeigt.
Fax Rufnr	Falls eine Faxbox eingerichtet ist (z. B. mit den UC Clients myPortal for Desktop oder myPortal for Outlook), hier die Fax-Rufnummer eintragen, unter der der Teilnehmer von intern Faxnachrichten empfangen kann.
Fax DuWa	Falls eine Faxbox eingerichtet ist (z. B. mit den UC Clients myPortal for Desktop oder myPortal for Outlook), hier die Fax-Rufnummer eintragen, unter der der Teilnehmer von extern Faxnachrichten empfangen kann.
Access	Anzeige der physikalischen Schnittstelle, an der das Endgerät angeschlossen ist.
Suche	Sie können sich auch ausgewählte Teilnehmer anzeigen lassen, indem Sie in die **Suche**-Felder den Suchbegriff eingeben und mit der Return-Taste bestätigen. Die zu dem Suchbegriff passenden Teilnehmer werden angezeigt. Sind alle **Suche**-Felder leer und wird die Return-Taste gedrückt, werden wieder alle Teilnehmer aufgelistet.
Einträge pro Seite	Auswahl, ob 10, 25, 50 oder 100 Einträge pro Seite angezeigt werden sollen.
Schaltflächen	
Blauer Pfeil in Spalte **Rufnr**	Ruft die Seite mit den Registerkarten **Teilnehmer-Parameter ändern**, **Teilnehmer-Flags ändern**, **Workpointclient Daten ändern** und **Gruppen/RWS ändern** auf.
>	Springt eine Seite weiter.

Parameter	Beschreibung
<	Springt eine Seite zurück.
>|	Springt zum Ende der Liste.
|<	Springt zum Anfang der Liste.

27.3.7.7 Teilnehmer > Teilnehmer > IVM/EVM Ports > IVM

Parameterbeschreibung der Registerkarten:

- **Teilnehmer ändern**

Parameter	Beschreibung
Rufnr	Interne Rufnummer des IVM-Ports.
DuWa	Durchwahlnummer des IVM-Ports, sofern vorhanden.
Name	Frei wählbarer Name des IVM-Ports. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Clip/Lin	Ziffernfolge, die beim einem gehenden externen Anruf beim Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird (z.B. für Notrufdienst E911 USA).
Aktiv	Zeigt an, ob der IVM-Port betriebsbereit ist.
Endgeräte Typ	Bei IVM wird S0-Teilnehmer angezeigt.
Access	Anzeige des internen Ports für die IVM.
Stationstyp	Für die IVM ist "Phonemail" zu wählen, für Ansagefunktion auf "Standard" stellen.
Parameter	Standardansicht für alle Teilnehmer, Einstellungen nicht verändern (z.B. "Sprache" ist nicht die Sprache der Voicemail-Ansagen).
Suche	Sie können sich auch ausgewählte IVM-Ports anzeigen lassen, indem Sie in die **Suche**-Felder den Suchbegriff eingeben und mit der Return-Taste bestätigen. Die zu dem Suchbegriff passenden IVM-Ports werden angezeigt. Sind alle **Suche**-Felder leer und wird die Return-Taste gedrückt, werden wieder alle IVM-Ports aufgelistet.
Einträge pro Seite	Auswahl, ob 10, 25, 50 oder 100 Einträge pro Seite angezeigt werden sollen.
Schaltflächen	
Blauer Pfeil in Spalte **Rufnr**	Ruft die Seite mit den Registerkarten **Teilnehmer-Parameter ändern**, **Teilnehmer-Flags ändern**, **Workpointclient Daten ändern** und **Gruppen/RWS ändern** auf.
>	Springt eine Seite weiter.
<	Springt eine Seite zurück.
>|	Springt zum Ende der Liste.
|<	Springt zum Anfang der Liste.

27.3.7.8 Teilnehmer > Teilnehmer > IVM/EVM Ports > EVM

Parameterbeschreibung der Registerkarten:

- **Teilnehmer ändern**

Parameter	Beschreibung
Rufnr	Interne Rufnummer des Voicemail-Ports.
DuWa	Durchwahlnummer des Voicemail-Ports, sofern vorhanden.
Name	Frei wählbarer Name des Voicemail-Ports. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Clip/Lin	Ziffernfolge, die beim einem gehenden externen Anruf beim Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird (z.B. für Notrufdienst E911 USA).
Aktiv	Zeigt an, ob der Voicemail-Port betriebsbereit ist.
Endgeräte Typ	Bei EVM wird S0-Teilnehmer angezeigt.
Access	Anzeige des internen Ports für die Voicemail.
Stationstyp	Für die EVM ist "Phonemail" zu wählen, für Company AutoAttendant auf "Standard" stellen.
Parameter	Standardansicht für alle Voicemail-Ports, Einstellungen nicht verändern (z.B. "Sprache" ist nicht die Sprache der Voicemail-Ansagen).
Suche	Sie können sich auch ausgewählte Voicemail-Ports anzeigen lassen, indem Sie in die **Suche**-Felder den Suchbegriff eingeben und mit der Return-Taste bestätigen. Die zu dem Suchbegriff passenden Voicemail-Ports werden angezeigt. Sind alle **Suche**-Felder leer und wird die Return-Taste gedrückt, werden wieder alle Voicemail-Ports aufgelistet.
Einträge pro Seite	Auswahl, ob 10, 25, 50 oder 100 Einträge pro Seite angezeigt werden sollen.
Schaltflächen	
Blauer Pfeil in Spalte **Rufnr**	Ruft die Seite mit den Registerkarten **Teilnehmer-Parameter ändern**, **Teilnehmer-Flags ändern**, **Workpointclient Daten ändern** und **Gruppen/RWS ändern** auf.
>	Springt eine Seite weiter.
<	Springt eine Seite zurück.
>|	Springt zum Ende der Liste.
|<	Springt zum Anfang der Liste.

27.3.7.9 Teilnehmer > Teilnehmer > Virtuelle Teilnehmer

Parameterbeschreibung der Registerkarten:

- **Teilnehmer ändern**

Parameter	Beschreibung
Rufnr	Interne Rufnummer des virtuellen Teilnehmers.
DuWa	Durchwahlnummer des virtuellen Teilnehmers.
Name	Frei wählbarer Name des virtuellen Teilnehmers. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Typ	Frei oder Virtueller Teilnehmer (bei Mobility Entry feste Anzeige)

Parameter	Beschreibung
Clip/Lin	Ziffernfolge, die beim einem gehenden externen Anruf beim Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird (z.B. für Notrufdienst E911 USA)
Aktiv	Zeigt an, ob der virtuelle Teilnehmer betriebsbereit ist.
Suche	Sie können sich auch ausgewählte Teilnehmer anzeigen lassen, indem Sie in die **Suche**-Felder den Suchbegriff eingeben und mit der Return-Taste bestätigen. Die zu dem Suchbegriff passenden Teilnehmer werden angezeigt. Sind alle **Suche**-Felder leer und wird die Return-Taste gedrückt, werden wieder alle Teilnehmer aufgelistet.
Einträge pro Seite	Auswahl, ob 10, 25, 50 oder 100 Einträge pro Seite angezeigt werden sollen.
Schaltflächen	
Blauer Pfeil in Spalte **Rufnr**	Ruft die Seite mit den Registerkarten **Teilnehmer-Parameter ändern**, **Teilnehmer-Flags ändern**, **Workpointclient Daten ändern** und **Gruppen/RWS ändern** auf.
>	Springt eine Seite weiter.
<	Springt eine Seite zurück.
>|	Springt zum Ende der Liste.
|<	Springt zum Anfang der Liste.

27.3.7.10 Teilnehmer > Teilnehmer > Teilnehmer-Parameter

Parameterbeschreibung der Registerkarten:

- **Teilnehmer-Parameter ändern**

Parameter	Beschreibung
Teilnehmer - ...	
Typ	Typ des Teilnehmers.
Rufnummer	Interne Rufnummer des Teilnehmers.
Name	Frei wählbarer Name des Teilnehmers. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Durchwahl	Durchwahlnummer des Teilnehmers.
Endgeräte Typ	Anzeige des dem Teilnehmer zugeodneten Endgeräts.
Clip/Lin	Ziffernfolge, die beim einem gehenden externen Anruf beim Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird (z.B. für Notrufdienst E911 USA) Wertebereich: max. 16 Ziffern
Access	Anzeige der physikalischen Schnittstelle, an der das Endgerät angeschlossen ist.
Fax	
Rufnummer	Falls eine Faxbox eingerichtet ist (z. B. mit den UC Clients myPortal for Desktop oder myPortal for Outlook), hier die Fax-Rufnummer eintragen, unter der der Teilnehmer von intern Faxnachrichten empfangen kann.

Parameter	Beschreibung
Durchwahl	Falls eine Faxbox eingerichtet ist (z. B. mit den UC Clients myPortal for Desktop oder myPortal for Outlook), hier die Fax-Rufnummer eintragen, unter der der Teilnehmer von extern Faxnachrichten empfangen kann.
Mobility	
Mobile Rufnummer	Nur für SIP-Clients und mobile Teilnehmer: Für One-Number-Service dient diese Rufnummer zur Authentifizierung des DISA-Zugangs per Mobilfunk. Geben Sie hier die zugehörige Mobilfunk-Rufnummer des Teilnehmers mit Amtskennziffer ein (z. B. 0017312345678).
Web Feature ID	Die Web Feature ID legt fest, wie sich der Teilnehmer am mobilen web Client einloggen soll (Benutzername). Auswahl zwischen "keine" (nur Mobility Entry) und "automatisch" (interne Rufnummer des Teilnehmers) oder Auswahl der Rufnummer des Clients bzw. des Telefons aus der Klappliste.
Parameter	
Stationstyp	Typ des angeschlossenen Endgeräts (Klappliste)
Stationstyp: **Standard**	Systemtelefone oder analoge Telefone
Stationstyp: **Fax**	Faxgerät, z.B. kein Aufschalten möglich
Stationstyp: **Lautsprecher**	Für eine über den a/b-Port realisierte Durchsageeinrichtung
Stationstyp: **Anrufbeantworter**	nur bei analog: ist an dieser Schnittstelle ein Anrufbeantworter angeschlossen, kann mit dieser Einstellung von jedem Endgerät ein Gespräch vom Anrufbeantworter übernommen werden, obwohl der Anrufbeantworter das Gespräch bereits angenommen hat. Dazu muss am Endgerät eine Taste mit der internen Rufnummer dieses analogen Teilnehmers programmiert werden. Dieser Eintrag sollte außer für Anrufbeantworter auch für virtuelle Ports gewählt werden, bei denen keine physikalischen Geräte eingerichtet sind. Hierdurch wird verhindert, dass das Kommunikationssystem den Port auf dessen Betriebszustand prüft. nur für virtuelle Ports: Wurde im Manager E ein Teilnehmer ohne Access als Typ Anrufbeantworter konfiguriert, muss der Port zusätzlich als virtueller Port konfiguriert sein. Ansonsten ist er im WBM nicht als Teilnehmer sichtbar.
Stationstyp: **Nofe MW-LED**	Für analoge Telefone (NoFe = Normalfernsprecher) mit Message Waiting-LED nicht für USA
Stationstyp: **Teilnehmer mit Impulsschleife**	Bei Verwendung eines Impulsschleifen-Endgerätes mit Türöffnerfunktion
Stationstyp: **Modem**	Bei dieser Einstellung ist kein Aufschalten möglich. Sie ist vorgesehen für Modems.
	Wenn ein Fax- oder Modem-Teilnehmer gelöscht wird (Ruf-Nr. und DuWa werden gelöscht), muss auch der Stationstyp wieder auf Standard gesetzt werden.
Sprache	Sprache für die Menüsteuerung des Endgeräts (Systemtelefons).
Rufsignalisierung intern	Hier können jedem Teilnehmer eine von insgesamt acht internen Rufsignalisierungen zugewiesen werden. Damit wird zusätzlich zu dem externen Rufton nun ein interner Rufton zugewiesen, der bei einem internen Anruf übertragen wird. Standardwert: Rufart 1

Parameter	Beschreibung
Rufsignalisierung extern	Hier können drei verschiedene Rufarten eingestellt werden, die einen externen Ruf signalisieren: – Systemtelefone Rufart 1 = Externruf Amt (z.B. Doppelruf) Rufart 2 = Externruf Amt 2 (z.B. Dreifachruf) Rufart 3 = Externruf Amt 3 (z.B. kurz/lang/kurz) – Analoge Endgeräte, Deutschland: Rufart 1 = Externruf Amt Rufart 2 = Wiederanruf Rufart 3 = Türklingelruf – Analoge Endgeräte, Andere Länder: Rufart 1 = Externruf Amt Rufart 2 = Externruf Amt Rufart 3 = Externruf Amt Standardwert: Rufart 1
Berechtigung (LCR)	Ein Teilnehmer kann einen Weg nur dann belegen, wenn seine Berechtigung größer oder gleich der LCR-Berechtigung in der Wegetabelle ist, das heißt ein Teilnehmer mit Berechtigung 7 kann einen Weg mit Berechtigung 8 nicht belegen. Standardmäßig sind alle Teilnehmer mit maximaler LCR-Berechtigung (15) eingetragen. Standardwert: 15
Hotline Modus	Auswahl der Hotline-Optionen
Hotline Modus: **aus**	Hotline-Funktion ausgeschaltet.
Hotline Modus: **Röcheln**	Der Ruf zur Hotline erfolgt nach einer vorgegebenen Wartezeit (Röchelzeit), siehe Telefonie/Grundeinstellungen/System/Abwurf-VPL-Hotline
Hotline Modus: **Hotline**	Hotline-Funktion eingeschaltet. Beim Abheben des Hörers wird sofort die Verbindung zum Hotlineziel aufgebaut, siehe Telefonie/Grundeinstellungen/System/Abwurf-VPL-Hotline
Hotline	Auswahl der Hotline-Ziele, siehe Telefonie/Grundeinstellungen/System/Abwurf-VPL-Hotline
Hotline: **keine**	kein Ziel definiert
Hotline: **Ziffern 1 bis 6**	Hotline-Ziele, siehe Telefonie/Grundeinstellungen/System/Abwurf-VPL-Hotline
Payload Security	Nur für IP System Clients: Aktivieren oder Deaktivieren der Verschlüsselung von Telefongesprächen (SPE). Dazu müssen alle beteiligten Teilnehmer SPE aktiviert haben.
Schaltflächen	
>	Springt zum nächsten Teilnehmer. Wurden zuvor über die **Suche**-Felder die zum eingegebenen Suchbegriff passenden Teilnehmer gefiltert, können nur diese Teilnehmer angesprungen werden.
<	Springt einen Teilnehmer zurück.

Parameterbeschreibung der Registerkarten:

- **Teilnehmer-Flags ändern**

Parameter	Beschreibung
Teilnehmer - ...	
Typ	Typ des Teilnehmers.
Rufnummer	Interne Rufnummer des Teilnehmers.
Name	Name des Teilnehmers.
Teilnehmer-Flags	

Parameter	Beschreibung
Aufschaltberechtigung ein	Bei aktiviertem Flag kann sich der Teilnehmer auf die bestehende Verbindung eines internen Teilnehmers aufschalten. Die beteiligten Teilnehmer werden durch einen Aufmerksamkeitston und durch eine Displaymeldung über das Aufschalten informiert. Standardwert: Deaktiviert
Anrufschutz durchbrechen	Bei aktiviertem Flag gilt: Trifft der Teilnehmer auf einen internen Teilnehmer mit aktiviertem Anrufschutz, kann er den Anrufschutz durchbrechen. Nach fünf Sekunden wird dem gerufenen Teilnehmer der Anruf signalisiert. Bei deaktivertem Flag kann der Anrufschutz nicht durchbrochen werden. Trifft der Teilnehmer auf einen internen Teilnehmer mit aktiviertem Anrufschutz, erhält er den Besetztton. Standardwert: Deaktiviert
AUL extern erlaubt	Bei aktiviertem Flag kann der Teilnehmer eine Anrufumleitung zu einem externen Ziel aktivieren. Die bei der Ausführung einer externen Anrufumleitung anfallenden Gebühren werden dem Teilnehmer zugewiesen, der die Anrufumleitung aktiviert hat. tandardwert: Aktiviert
Direktansprechschutz aus	Bei aktiviertem Flag kann der Teilnehmer direkt angesprochen werden. Ermöglicht wird damit ein interner Verbindungsaufbau, ohne dass der Teilnehmer den Hörer abhebt. Der Lautsprecher des Teilnehmers wird dabei automatisch eingeschaltet. Standardwert: Aktiviert
DISA Berechtigung	Bei aktiviertem Flag kann der Teilnehmer von extern über DISA (Direct Inward System Access) – wie als interner Teilnehmer – Funktionen des Kommunikationssystems aktivieren oder deaktivieren und gehende externe Verbindungen aufbauen. Dazu gehört zum Beispiel das Aktivieren und Deaktivieren einer Anrufumleitung, des Anrufschutzes und des Codeschlosses. Standardwert: Deaktiviert
Transit schalten durch Auflegen	Bei aktiviertem Flag kann der Teilnehmer ein externes Gespräch an einen anderen externen Teilnehmer durch Auflegen übergeben. Beispiel: Der Teilnehmer ist Konferenzleiter und legt auf: Verbleiben interne Teilnehmer in der Konferenz, wird der am längsten teilnehmende interne Teilnehmer automatisch zum Konferenzleiter. Verbleiben ausschließlich externe Teilnehmer in der Konferenz, wird die Konferenz beendet und alle Verbindungen werden getrennt. Standardwert: Deaktiviert
Codeschloss zurücksetzen	Bei aktiviertem Flag kann der Teilnehmer das individuelle Codeschloss anderer interner Teilnehmer auf den Standardcode zurücksetzen. Standardwert: Deaktiviert
Kommendes CLIP für Analog (nur für analoge Teilnehmer)	Bei aktiviertem Flag wird im Telefondisplay des analogen Teilnehmers die Rufnummer des Anrufers angezeigt. Voraussetzung dafür ist, das das analoge Telefon des Teilnehmers CLIP (Calling Line Identification Presentation) unterstützt. Standardwert: Aktiviert

Parameter	Beschreibung
Zugriff für Fangen	Bei aktiviertem Flag kann der Teilnehmer unerwünschte externe Anrufer über das ISDN-Amt identifizieren lassen. Voraussetzung dafür ist, dass die Freischaltung der Leistungsmerkmals "Fangen" (Malicious Call Identification MCID) beim Netzbetreiber beantragt wurde und erfolgt ist. Nach der Freischaltung des Leistungsmerkmals "Fangen" durch den Netzbetreiber ist folgendes zu beachten: Bei jeder kommenden Verbindung vom ISDN-Amt wird nach Auflegen des Anrufers das Auslösen der Verbindung zum gerufenen Teilnehmer für eine bestimmte Zeit verzögert, damit dieser das Leistungsmerkmal "Fangen" aktivieren kann. Dadurch wird die Verfügbarkeit der ISDN-Amtsleitungen reduziert. Standardwert: Deaktiviert
Eintrag in Telefonbuch	Bei aktiviertem Flag werden Name und Rufnummer des Teilnehmers im Systemtelefonbuch angezeigt. Standardwert: Aktiviert
Editieren der Wahl	Bei aktiviertem Flag kann der Teilnehmer die über die Wähltastatur eingegebenen Ziffern der Rufnummer vor der Wahlaussendung ändern (editieren). Voraussetzung dafür ist ein Systemtelefon mit Display. Standardwert: Deaktiviert
Keine Rufzuschaltung bei besetzt	Bei aktiviertem Flag gilt: Der Zustand des rufzuschaltenden Teilnehmers bestimmt, ob eine Rufzuschaltung durchgeführt wird: Der rufzuschaltende Teilnehmer ist frei: Alle zugeschalteten Teilnehmer werden sofort gerufen. Beim rufzuschaltenden Teilnehmer kann angeklopft werden: Alle zugeschalteten Teilnehmer werden nach 5 Sekunden gerufen. Beim rufzuschaltenden Teilnehmer kann nicht angerufen oder angeklopft werden: Es erfolgt keine Rufzuschaltung. Standardwert: Deaktiviert
Assoziierte Wahl/Dienste	Assoziierte Wahl: Bei aktiviertem Flag kann der Teilnehmer für einen anderen internen Teilnehmer eine Rufnummer wählen, so als würde der andere Teilnehmer selbst wählen. Assoziierte Dienste: Bei aktiviertem Flag kann der Teilnehmer für einen anderen internen Teilnehmer Leistungsmerkmale steuern, so als würde der andere Teilnehmer die Leistungsmerkmale selbst steuern. Dazu gehört zum Beispiel das Aktivieren und Deaktivieren einer Anrufumleitung, einer Rufzuschaltung und des Codeschlosses. Standardwert: Deaktiviert
Anklopfschutz ein	Bei aktiviertem Flag gilt: Führt der Teilnehmer ein Gespräch, erhält er keine Informationen über weitere kommende Anrufe mittels Anklopfton und Displaymeldung. Standardwert: Aktiviert
Diskretes Ansprechen	Bei aktiviertem Flag kann sich der Teilnehmer in die bestehende Gesprächsverbindung eines internen Teilnehmers einschalten. Er kann unbemerkt mithören und mit dem internen Teilnehmer sprechen, ohne dass der andere Teilnehmer dies hört. Voraussetzung dafür ist, dass es sich um eine Zweierverbindung handelt. Bei Rückfragegesprächen oder Konferenzen ist kein diskretes Ansprechen möglich. Standardwert: Deaktiviert
Schutz Diskretes Anspr.	Bei aktiviertem Flag kann der Teilnehmer nicht diskret angesprochen werden. Standardwert: Deaktiviert

Parameter	Beschreibung
DTMF-basierte Leistungsmerkmalaktivierung	Nur relevant für Mobility Entry Teilnehmer: Um im Gesprächszustand Leistungsmerkmale aktivieren zu können, muss dieses Flag gesetzt sein (Code Receiver bleibt aktiv, Achtung: begrenzte Ressourcen) Standardwert: Deaktiviert
Kopfsprechgarnitur	Bei aktiviertem Flag kann beim Teilnehmer eine Kopfsprechgarnitur am Handapparat-Anschluss angeschlossen werden. Das Flag bewirkt, dass man Anrufe durch Drücken einer Headset-Taste am Systemtelefon bei aufliegendem Handapparat entgegennehmen kann. Der Einsatz einer Kopfsprechgarnitur am Headset-Anschluss eines Systemtelefons wird vom Kommunikationssystem automatisch erkannt, eine Berechtigungsfreigabe ist hier nicht erforderlich. Ist dieses Flag aktiviert, können Anrufe nicht über die Lautsprecher-Taste ausgelöst werden; es muss dann für das Auslösen von Verbindungen eine Trennen-Taste programmiert werden. Standardwert: Deaktiviert
Vertretermailbox aktiv	Ist das Flag aktiviert und ist der Angerufene nicht erreichbar, dann wird der Anruf auf die Mailbox des Vertreters umgeleitet und die Rufnummer des Anrufenden wird am Display des Vertreter-Endgeräts angezeigt. Standardwert: Deaktiviert
Anrufprio./Sof. Freiton Anklopfen	Bei aktiviertem Flag (Anrufpriorität/Sofortiger Freiton bei Anklopfen) werden Anrufe durch diesen Teilnehmer mit höherer Priorität beim Partner signalisiert. Die Priorität wird dabei gleich gesetzt mit der Priorität von externen Anrufen. Die priorisierten Anrufe werden somit vor bestehende Internrufe, jedoch nach bestehenden Externanrufen eingereiht. Dabei ist zu beachten, dass bestehende Erstanrufe (nicht anklopfende Rufe) unabhängig von ihrer Rufart generell nicht verdrängt werden. Soll auch bei einem internen Anruf in einen anderen Knoten die Priorität entsprechend gesetzt werden, muss zusätzlich auch für die entsprechende Leitung das Leitungsflag "Anrufprio./Sof. Freiton Anklopfen" (Bereich Leitung Flags, Anrufprio./Sof. Freiton Anklopfen) gesetzt sein. Ist dieses Flag gesetzt, bekommt der Anrufer beim Anklopfen einen sofortigen Freiton anstatt des Besetzttons. Dieses hat keinen Einfluss auf die akustische Signalisierung. Die priorisierten Anrufe werden weiterhin wie ein Internruf signalisiert. Dieses Leistungsmerkmal ist wichtig z.B. bei Phonemail-Anschlüssen. Standardwert: Deaktiviert
Sprachaufzeichnung	Bei aktiviertem Flag kann der Teilnehmer während eines Gesprächs die Sprachaufzeichnung aktivieren. Über Flags, Schalter "Hinweiston bei Sprachaufzeichnung" kann zusätzlich angegeben werden, ob während der Sprachaufzeichnung ein Hinweiston ausgegeben werden soll. Unter PhoneMail muss ein geeignetes Live Recording Aufnahmegerät eingerichtet sein. Wenn für die Sprachaufzeichnung die IVM verwendet werden soll, kann über "IVM | Weitere Einstellungen/Allgemein" die max. Länge der Sprachaufzeichnung eingestellt werden und angegeben werden, ob vor der Sprachaufzeichung eine entsprechende Signalisierung gemacht werden soll. Standardwert: Deaktiviert

Parameter	Beschreibung
Display-Ausgaben komprimieren	Bei aktiviertem Flag werden die Display-Ausgaben zum Zweck einer besseren Performance komprimiert. Ändert sich die Displayanzeige an einem UP0/E-Endgerät, aktualisiert das Kommunikationssystem nur die Daten, die sich von der vorhergehenden Anzeige unterscheiden. Bei Anschluss einer Anwendung (z.B. Smartset/TAPI) über einen RS-232-Adapter (Data- bzw. Control-Adapter) muss dieses Leistungsmerkmal deaktiviert sein. Bei Applikationen, die die Rufnummerninformation aus der Displayanzeige des Endgerätes beziehen, muss das Flag deaktiviert werden (d.h. unkomprimierte Ausgabe mit Rufnummer statt komprimierter Ausgabe mit Namen). Namen werden generell nur angezeigt, wenn unter Display "Name/Rufnummer anzeigen" das Flag "nur Rufnummer" deaktiviert ist. Standardwert: Aktiviert
Türfreigabe, DTMF	Bei aktiviertem Flag kann der Teilnehmer mittels DTMF/MFV-Code die Tür öffnen, wenn am betreffenden Port ein Tür-Relais angeschlossen ist. Standardwert: Deaktiviert
Autom. Rufannahme, CSTA (nur für OpenStage-SIP-Telefone)	Bei aktiviertem Flag gilt: Bei der Wahl oder der Rufannahme über myPortal oder myAttendant wird am zugehörigen SIP-Telefon der Freisprechmodus aktiviert. Die Angaben in der Dokumentation des SIP-Telefons sind zu beachten, da für die einwandfreie Nutzung des Leistungsmerkmals eventuell zusätzliche Einstellungen am SIP-Telefon notwendig sind. Bei deaktiviertem Flag erfolgt der Gesprächsaufbau erst nach Abnehmen des Hörers. Standardwert: Aktiviert
Call Monitoring (nur für bestimmte Länder)	Bei aktiviertem Flag kann der Teilnehmer das Gespräch eines beliebigen internen Teilnehmers mithören. Das Mikrofon des mithörenden Teilnehmers wird automatisch stummgeschaltet. Eine Information der überwachten Teilnehmer mittels Signalton oder Displayanzeige erfolgt nicht. Beim Beginn und beim Beenden von Call Monitoring können Gesprächsaussetzer von bis zu zwei Sekunden auftreten. Standardwert: Deaktiviert
Handsfree Mikrofon sperren	Bei aktiviertem Flag ist die Nutzung des Freisprechmikrofons nicht möglich. Das Flag wird ausschließlich durch OpenStage-Telefone unterstützt. Standardwert: Deaktiviert
Nummer Anzeige Erzwingen	Bei aktiviertem Flag wird anstelle des Namens die Rufnummer des rufenden Teilnehmers im Display des gerufenen Teilnehmers angezeigt. Standardwert: Deaktiviert
Nutzung (nur für bestimmte Länder)	Mit dieser Aufklappliste kann der Ausgangsstrom der Schnittstellen einer analogen Baugruppe konfiguriert werden (in mA, z. B. 27 mA für China)
Aktueller Betriebszustand	In dieser Klappliste kann eine Betriebsart des Teilnehmeranschlusses ausgewählt werden.
Payload Sicherheit (nur für TDM-Systemtelefone)	Ist dieses Flag sowie das Systemflag **SPE Unterstützung** aktiviert, wird Signaling & Payload Encryption (SPE) für den (die) ausgewählten Teilnehmer unterstützt. Dabei werden die Signalisierungs- und Sprachdaten für diese(n) Teilnehmer verschlüsselt. Es kann eingestellt werden, ob im Display angezeigt werden soll, wenn ein Teil des Verbindungsweges zu einem IP-Teilnehmer verschlüsselt wird (Off = Es erfolgt keine Anzeige im Display). Für alle anderen Endgeräte ist die Einstellung der Payload-Sicherheit ohne Funktion. Standardwert: Deaktiviert

Parameter	Beschreibung
Schaltflächen	
>	Springt zum nächsten Teilnehmer. Wurden zuvor über die **Suche**-Felder die zum eingegebenen Suchbegriff passenden Teilnehmer gefiltert, können nur diese Teilnehmer angesprungen werden.
<	Springt einen Teilnehmer zurück.

Parameterbeschreibung der Registerkarten:

- **Workpointclient Daten ändern**

Parameter	Beschreibung
Teilnehmer - ...	
Typ	Typ des Teilnehmers.
Rufnummer	Interne Rufnummer des Teilnehmers.
Name	Name des Teilnehmers.
Parameter	
Status Message	Nur für System-Clients: Dieses Flag aktiviert den “keep-alive”-Mechanismus für Systemtelefone. Fällt ein Systemtelefon z. B. aus, so wird nach 4 Minuten dieses Systemtelefon als inaktiv gekennzeichnet. Beim Einrichten eines Systemtelefons als Heimarbeitsplatz sowie bei der Nutzung des Leistungsmerkmals “Short Hold” darf das Flag nicht aktiviert sein. Wenn dieses Flag nicht aktiviert ist, wird der Meldungsverkehrs zwischen dem Kommunikationssystem und den Systemtelefonen reduziert.
Authentifizierung aktiv	Soll sich der IP-Client am Kommunikationssystem mit einem Kennwort identifizieren, muss die Authentifizierung aktiviert und ein Kennwort vergeben werden. Dies ist insbesondere bei Clients von Vorteil, die nicht im internen LAN liegen, sondern sich von außen einwählen.
Neues Kennwort	Kennwort für die Authentifizierung.
Kennwort bestätigen	Kennwort für die Authentifizierung wiederholen.
SIP User ID / Benutzername	Nur für SIP-Clients: Frei wählbarer Benutzernamen für die Authentifizierung des SIP-Teilnehmers, z. B. "SIP-120". Der hier definierte Wert muss auch am SIP-Telefon eingegeben werden.
Realm	Nur für SIP-Clients: frei wählbarer Namen für die zugehörige Zone, z. B. "OSBIZ-SIP". Dieser Wert muss für alle SIP-Clients gleich sein. Der hier definierte Wert muss auch am SIP-Telefon eingegeben werden.
Feste IP Adresse verwenden	Nur für SIP-Clients: Die Eingabe einer festen IP Adresse stellt sicher, dass sich nur ein SIP-Client mit dieser IP Adresse am System anmelden kann. Wenn dieses Flag aktiviert wird, werden die IP Adresse und die Rufnummer überprüft. Ist das Flag nicht aktiviert, wird nur die Rufnummer überprüft.
IP Adresse	Nur für SIP-Clients: IP-Adresse des SIP-Clients (z.B. die IP-Adresse des SIP-Telefons)
Typ	Nur für System-Clients: Ein mobiler IP Client (Option Mobil) ist keinem IP Telefon fest zugeordnet. Mit der Rufnummer eines mobilen IP Clients kann sich ein Teilnehmer über die Anmeldeprozedur (*9419) an jedem IP-Endgerät anmelden, das dieses erlaubt (Option Mobil blockiert ist nicht aktiviert).
Typ: **Mobil**	Nur für System-Clients: Dem Teilnehmer ist kein IP-Endgerät fest zugeordnet. Das Leistungsmerkmal wird erst ab dem 3. Teilnehmerport unterstützt.

Parameter	Beschreibung
Typ: **Nicht mobil**	Nur für System-Clients: Dem IP-Endgerät des Teilnehmers ist die Rufnummer fest zugeordnet. Bei Einsatz eines WLx-Phones muss die Option Nicht mobil gesetzt sein, bevor das WLx- Phone am Kommunikationssystem registriert ist.
Typ: **Nicht mobil und blockiert**	Nur für System-Clients: Ein Teilnehmer kann sich nicht mit einem mobilen System-Client an diesem IP-Endgerät anmelden.
Blockiert für Deskshare-Teilnehmer	Nur für System-Clients: dieses System-Telefon können sich mehrere Teilnehmer teilen (DeskSharing).
ID des Sekundärsystems	Dieser Parameter hat zwei unterschiedliche Funktionalitäten: 1. Für alle Teilnehmer: definiert das dem Teilnehmer zugeordnete Multi-Location-Gateway. 2. Nur für System-Clients: Ist bei vernetzten Systemen das Flag "Notbetrieb" gesetzt (unter "Teilnehmer/IP Clients/Sekundäres Gateway"), kann hier die Knoten-ID des Ausfallsystems für System-Clients eingetragen werden.
Internet-Registrierung am internen SBC	Aktiviert das Leistungsmerkmal SIP@Home. Damit kann sich ein externes STUN-fähiges SIP-Telefon über das Internet an OpenScape Business registrieren und wie ein internes Telefon genutzt werden.
Schaltflächen	
>	Springt zum nächsten Teilnehmer. Wurden zuvor über die **Suche**-Felder die zum eingegebenen Suchbegriff passenden Teilnehmer gefiltert, können nur diese Teilnehmer angesprungen werden.
<	Springt einen Teilnehmer zurück.

Parameterbeschreibung der Registerkarten:

- **Gruppen/RWS ändern**

Parameter	Beschreibung
Teilnehmer - ...	
Typ	Typ des Teilnehmers.
Rufnummer	Interne Rufnummer des Teilnehmers.
Name	Name des Teilnehmers.
Rufweiterschaltung	
Ziel Tag	Anzeige der Rufweiterschaltungsziele für kommende externe Rufe am Tag (siehe Wizard User-Telefonie/Rufweiterschaltung)
Ziel Nacht	Anzeige der Rufweiterschaltungsziele für kommende externe Rufe in der Nacht (siehe Wizard User-Telefonie/Rufweiterschaltung).
Ziel Intern	Anzeige der Rufweiterschaltungsziele für kommende interne Rufe (siehe Wizard User-Telefonie/Rufweiterschaltung).
Berechtigung	
Tag	Jedem Teilnehmer kann eine Berechtigungsklasse für den Tag zugeordnet werden. Es kann zwischen 15 Berechtigungsklassen gewählt werden (siehe Telefonie/Berechtigungen).

Parameter	Beschreibung
Nacht	Jedem Teilnehmer kann eine Berechtigungsklasse für die Nacht zugeordnet werden. Es kann zwischen 15 Berechtigungsklassen gewählt werden (siehe Telefonie/Berechtigungen).
Anrufübernahme	
Gruppe	Jeder Teilnehmer kann einer Anrufübernahmegruppe zugeordnet werden. Es kann zwischen 32 Anrufübernahmegruppen ausgewählt werden (siehe Kommende Rufe / Anrufübernahme).
Schaltflächen	
>	Springt zum nächsten Teilnehmer. Wurden zuvor über die **Suche**-Felder die zum eingegebenen Suchbegriff passenden Teilnehmer gefiltert, können nur diese Teilnehmer angesprungen werden.
<	Springt einen Teilnehmer zurück.

27.3.7.11 Teilnehmer > Teilnehmer > Applikation-Suite

Hier sind die Funktionen der UC Suite dargestellt. Es wird empfohlen, die Grundeinstellungen unter "Einrichtung > Grundinstallation > Basisinstallation > Vorkonfigurierte Rufnummern ändern" vorzunehmen.

Parameterbeschreibung der Registerkarten:

- **Teilnehmer ändern**

Parameter	Beschreibung
Rufnr	Rufnummer des Dienstes
DuWa	Durchwahlnummer des Dienstes
Name	Frei wählbarer Name des Dienstes Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Typ	Auto-Attendant / Fax / Contact Center Fax / Parken / MeetMe / Konferenz / Fax Gruppe
Clip/Lin	Ziffernfolge, die beim einem gehenden externen Anruf beim Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird (z.B. für Notrufdienst E911 USA)
Aktiv	Zeigt an, ob der Dienst betriebsbereit ist.
Suche	Sie können sich auch ausgewählte Dienste anzeigen lassen, indem Sie in die **Suche**-Felder den Suchbegriff eingeben und mit der Return-Taste bestätigen. Die zu dem Suchbegriff passenden Dienste werden angezeigt. Sind alle **Suche**-Felder leer und wird die Return-Taste gedrückt, werden wieder alle Dienste aufgelistet.
Einträge pro Seite	Auswahl, ob 10, 25, 50 oder 100 Einträge pro Seite angezeigt werden sollen.
Schaltflächen	
Blauer Pfeil in Spalte **Rufnr**	Ruft die Seite mit den Registerkarten **Teilnehmer-Parameter ändern**, **Teilnehmer-Flags ändern**, **Workpointclient Daten ändern** und **Gruppen/RWS ändern** auf.
>	Springt eine Seite weiter.

Parameter	Beschreibung
<	Springt eine Seite zurück.
>|	Springt zum Ende der Liste.
|<	Springt zum Anfang der Liste.

27.3.7.12 Teilnehmer > Teilnehmer > Profile/Vorlagen

Hier können Benutzerprofile (Teilnehmer-Parameter, Teilnehmer-Flags, Gruppen/ RWS) eingerichtet werden, so dass auf einfache Weise eine Grundeinstellung für viele Benutzer zugleich entsteht.

Parameterbeschreibung der Registerkarten:

- **Alle Profile bearbeiten**

Parameter	Beschreibung
Profile	Anzeige der Profilnummer.
Name	Eingabe eines beliebigen Profilnamens.

Parameterbeschreibung der Registerkarten:

- **Alle Profile Mitglieder anzeigen**

Parameter	Beschreibung
Profile	Anzeige der Profilnummer.
Name	Anzeige des Profilnamens.
Mitglied Rufnr	Anzeige der internen Rufnummer des Profil-Mitglieds.
Mitglied Name	Anzeige des Namens des Profil-Mitglieds.

Parameterbeschreibung der Registerkarten:

- **Profile Mitglied hinzufügen/löschen**

Parameter	Beschreibung
Profile - ...	Anzeige der Profilnummer.
Name	Anzeige des vergebenen Profilnamens.
Profile Mitglieder	
Auswahl	Liste der im System verfügbaren Teilnehmer.
Mitglieder	Liste der dem Profil zugeordneten Teilnehmer.
Schaltflächen	
Hinzufügen	Markierten Teilnehmer aus der Auswahl in die Liste der Profil-Mitglieder übernehmen.
Löschen	Markiertes Mitglied aus der Liste der Profil-Mitglieder löschen.

Parameterbeschreibung der Registerkarten:

- **Profil importieren/exportieren**

Parameter	Beschreibung
Profil über HTTP laden	
Remote-Dateiname (PC-Dateisystem)	Laden einer bereits vorhandenen Profil-Datei im XML-Format-
Profil über HTTP exportieren	
Dateiname	Anzeige des Dateinamens, unter dem das Profil ausgegeben wird (Format XML)
Aktion	Download des Profils
Schaltflächen	
Default-Werte zurücksetzen	Die Profilwerte für alle diesem Profil zugewiesenen Teilnehmer werden auf den Defaultwert zurückgesetzt.

Parameterbeschreibung der Registerkarten:

- **Import/Export alle Profile**

Parameter	Beschreibung
Alle Profile über HTTP laden	
Remote-Dateiname (PC-Dateisystem)	Laden einer bereits vorhandenen Profil-Datei. In dieser Datei können auch mehrere Profile gespeichert sein.
Alle Profile über HTTP exportieren	
Dateiname	Anzeige des Dateinamens, unter dem die Profile abgespeichert werden.
Aktion	Download der Profile in eine Profil-Datei.
Schaltflächen	
Default-Werte zurücksetzen	Die Profilwerte für alle Profile und zugewiesene Teilnehmer werden auf den Defaultwert zurückgesetzt.

Parameterbeschreibung der Registerkarten:

- **Teilnehmer-Parameter ändern: siehe Teilnehmer > Teilnehmer > Teilnehmer-Parameter**
- **Teilnehmer-Flags ändern: siehe Teilnehmer > Teilnehmer > Teilnehmer-Parameter**
- **Gruppen/RWS ändern: siehe Teilnehmer > Teilnehmer > Teilnehmer-Parameter**

27.3.7.13 Teilnehmer > Teilnehmer > Durchwahl Rufnummern

Hier wird eine Übersicht der konfigurierten Durchwahl-Rufnummern mit den zugehörigen Teilnehmern angezeigt.

Parameterbeschreibung der Registerkarten:

- **Durchwahl Rufnummern anzeigen**

Parameter	Beschreibung
Rufnr	Rufnummernanzeige des Teilnehmers.
Name	Namensanzeige des Teilnehmers.
DuWa	Durchwahlnummernanzeige des Teilnehmers.
(weitere Felder können angezeigt werden)	

27.3.7.14 Teilnehmer > Teilnehmer > Mobility Entry

Es wird empfohlen, mobile Teilnehmer über den Wizard "User Telefonie > Mobiltelefon Integration" einzurichten.

Parameterbeschreibung der Registerkarten:

- **Teilnehmer ändern**

Parameter	Beschreibung
Rufnr	Eingabe der internen Rufnummer des Mobility-Teilnehmers (z. B. 777). Diese interne Rufnummer darf noch nicht vergeben sein.
DuWa	Eingabe der internen Durchwahlnummer des Mobility-Teilnehmers. Diese interne Durchwahlnummer darf noch nicht vergeben sein.
Name	Eingabe eines beliebigen internen Namens des Mobility-Teilnehmers.
Typ	Anzeige des Typs des Mobility-Teilnehmers.
Mobile Rufnr	Eingabe der Rufnummer des Mobiltelefons. Eingabe mit führender Amtskennziffer, z.B. 0016012345678.
Web Feature ID	Die Web Feature ID legt fest, wie sich der Teilnehmer am mobilen web Client einloggen soll (Benutzername). Auswahl zwischen "keine" (nur Mobility Entry) und "automatisch" (interne Rufnummer des Teilnehmers) oder Auswahl der Rufnummer des Clients bzw. des Telefons aus der Klappliste.
Suche	Sie können sich auch ausgewählte Teilnehmer anzeigen lassen, indem Sie in die **Suche**-Felder den Suchbegriff eingeben und mit der Return-Taste bestätigen. Die zu dem Suchbegriff passenden Teilnehmer werden angezeigt. Sind alle **Suche**-Felder leer und wird die Return-Taste gedrückt, werden wieder alle Teilnehmer aufgelistet.
Einträge pro Seite	Auswahl, ob 10, 25, 50 oder 100 Einträge pro Seite angezeigt werden sollen.
Schaltflächen	
Blauer Pfeil in Spalte **Rufnr**	Ruft die Seite mit den Registerkarten **Teilnehmer-Parameter ändern**, **Teilnehmer-Flags ändern**, **Workpointclient Daten ändern** und **Gruppen/RWS ändern** auf.
>	Springt eine Seite weiter.
<	Springt eine Seite zurück.
>|	Springt zum Ende der Liste.
|<	Springt zum Anfang der Liste.

Parameterbeschreibung der Registerkarten:

- **Sekundäres Gateway**
  Nur für vernetzte Systeme (Multi-Location)

Parameter	Beschreibung
Rufnummer	Interne Rufnummer des Mobility-Teilnehmers.
Name	Name des Mobility-Teilnehmers.
Node-ID	Eintrag der Knoten-ID, über die der mobile Teilnehmer extern erreichbar ist.

27.3.7.15 Teilnehmer > Teilnehmer > Übersicht Teilnehmer

Listet alle Teilnehmer des Kommunikationssystems auf sortiert nach der Rufnummer (Standard). Ein Klick auf einen anderen Spaltentitel sortiert die Liste nach der gewählten Spalte aufsteigend, ein weiterer Klick absteigend.

Parameterbeschreibung der Registerkarten:

- **Teilnehmer ändern**

Parameter	Beschreibung
Rufnr	Interne Rufnummer des Teilnehmers.
DuWa	Durchwahlnummer des Teilnehmers.
Name	Frei wählbarer Name des Teilnehmers. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Endgeräte Typ	Anzeige des Typs des Teilnehmers.
Aktiv	Zeigt an, ob der Teilnehmer betriebsbereit ist.
Zugang	Anzeige der physikalischen Schnittstelle, an der das Endgerät angeschlossen ist.
Suche	Sie können sich auch ausgewählte Teilnehmer anzeigen lassen, indem Sie in die **Suche**-Felder den Suchbegriff eingeben und mit der Return-Taste bestätigen. Die zu dem Suchbegriff passenden Teilnehmer werden angezeigt. Sind alle **Suche**-Felder leer und wird die Return-Taste gedrückt, werden wieder alle Teilnehmer aufgelistet.
Einträge pro Seite	Auswahl, ob 10, 25, 50 oder 100 Einträge pro Seite angezeigt werden sollen.
Schaltflächen	
Blauer Pfeil in Spalte **Rufnr**	Ruft die Seite mit den Registerkarten **Teilnehmer-Parameter ändern**, **Teilnehmer-Flags ändern**, **Workpointclient Daten ändern** und **Gruppen/RWS ändern** auf.
>	Springt eine Seite weiter.
<	Springt eine Seite zurück.
>|	Springt zum Ende der Liste.
|<	Springt zum Anfang der Liste.

27.3.7.16 Teilnehmer > Tastenprogrammierung

Parameterbeschreibung der Registerkarten:

- **Tasten programmieren**
  Die Tastenprogrammierung wird nur für UP0-Telefone und HFA-Clients unterstützt.

Parameter	Beschreibung
Auswahlliste	Auswahl Telefons der Teilnehmers.
Ebenenumschaltung	Wenn eine Taste mit der Funktion "Ebenenumschaltung" eingerichtet wurde, kann hier die zweite Ebene programmiert werden
Telefon	Ein Klick auf den Tastenbereich des Telefons öffnet die aktuelle Tastenbelegung.
Tastenfeld	Anzeige der Tastenfunktion (Tastenbeschriftung)
Tastenschaltfläche	Auswahl der gewünschten Funktion

Parameterbeschreibung der Registerkarten:

- **Tastenlayout übernehmen**

Parameter	Beschreibung
Übernehme die Tastenkonfiguration vom Teilnehmer	Auswahl des Teilnehmers, dessen Tastenkonfiguration für ausgewählte Teilnehmer übernommen werden soll.
alle Teilnehmer	Tastenkonfiguration für alle Teilnehmer übernehmen.
Auswahlfeld	Übernahme der Tastenkonfiguration nur für die ausgewählten Teilnehmer
Station	Anzeige der internen Rufnummer und des Namens des Teilnehmers.
Device Type	Anzeige des Telefontyp des Teilnehmers.

27.3.8 Cordless

Unter **Cordless** sind die Funktionen für die integrierte Cordless-Lösung zum Betrieb von Cordless-Telefonen (DECT-Telefonen) über das Kommunikationssystem zusammengefasst. Hier werden die Basisstationen und die DECT-Telefone (interne Teilnehmer mit HFA-Leistungsmerkmalen) konfiguriert.

27.3.8.1 Cordless > Systemweit

Parameterbeschreibung der Registerkarten:

- **Systemweite Daten ändern**

Parameter	Beschreibung
CMI Daten	
Systemkennung	Eingabe der 8-stelligen, hexadezimalen DECT-Systemkennung. Diese wird beim Erwerb des DECT-Systems mit ausgeliefert. Sie setzt sich folgendermaßen zusammen: 1. Ziffer: E/ARC (Access Right Class) 2.-5. Ziffer: EIC (Equipment Installers Code) 6.-7. Ziffer: (FPN Fixed Part Number) 8. Ziffer: (FPS Fixed Part Subscriber)
Frequenzband	Auswahl des länderabhängigen Frequenzbandes. Es wird standardmäßig das dem eingetragenen Länderkennzeichen zugeordnete Frequenzband angezeigt.
Speech Coding	Anzeige des systemweiten Sprach-Codecs (a-law, µ-law).
Encryption	Encryption ist die Verschlüsselung der Daten auf der Luft-Schnittstelle und kann ein- oder ausgeschaltet werden. Standard: Aktiv
Anmeldefenster	Öffnungszeit des Anmeldefensters für die Anmeldung der DECT-Telefone. Das Anmeldefenster wird geöffnet, indem an einem Systemtelefon die Kennzahl *94 2 19970707 und das Passwort eingegeben wird. Anschließend werden im Anmeldefenster die Rufnummern der anzumeldenden DECT-Telefone eingegeben. Standard: 10 Minuten
Echo Handling Diese Parameter können die unter **Leitungen > Parameter/Allgemeine Flags** eingestellten Echo-Behandlungen für Mobilteilnehmer knotenweit außer Kraft setzen. Die Einstellung erfolgt nach der Leitungseinstellung der Gespräche. Eine Verbesserung durch generelle Deaktivierung oder leitungsspezifische Aktivierung muss im Einzelfall ausgetestet werden.	
Echo Suppressor	Der Echo Suppresssor (ES) schaltet abhängig vom Sendepegel des DECT-Telefons eine Dämpfung in Empfangsrichtung des DECT-Telefons. Wenn der Echo Suppressor eingeschaltet ist, kann es bei lauten Nebengeräuschen vorkommen, dass das Empfangssignal zusätzlich bedämpft wird. Dadurch wird die Verständigung zusätzlich erschwert. Im Modus **Deaktiv** wird die Empfangsrichtung des DECT-Telefons bei lautem Sendepegel des DECT-Telefons nicht bedämpft. Diese Einstellung kann bei analoger Amtsanschaltung und lauter Umgebung bessere Verständlichkeit des Amtsteilnehmers am DECT-Telefons bieten. Standard: Automatisch
Echo Canceller	Der Echo Canceller (EC) beseitigt unerwünschte Signalrückflüsse, die durch eine 4/2-Draht- Umsetzung (Gabel) im Festnetz verursacht werden. Bei aktiviertem Echo Canceller ohne Echo kann es zu Fehlern kommen, da der Echo Canceller versucht sich auf ein nicht vorhandenes Echo zu adaptieren. Im Modus **Deaktiv** wird das Schalten dieses Parameters verhindert und der Echo Canceller ist immer aus. Standard: Automatisch

Parameter	Beschreibung
Artificial Echo	Über den Artificial Echo-Weg (AE) wird ein Sprachsignal aus dem Festnetz zum fernen Teilnehmer um 24dB bedämpft zurückgeleitet. Dies kann notwendig sein, um ggf. (z.B. Internationale Verbindung) einem eingefügten Echo Canceller eine gewisse Vorlast zu geben. Im Modus **Deaktiv** wird das Schalten dieses Parameters verhindert und der Artificial Echo ist immer aus. Standard: Automatisch
PP Deviation Control	Bei VoIP-Verbindungen über DECT-Telefone treten oft Echos auf. Zum Unterdrücken/ Minimieren dieser Echos kann die Funktion „PP Deviation Control“ aktiviert werden. Diese Funktion wirkt auf alle an das Kommunikationssystem angeschlossenen DECT-Mobilteile. Für ein Mobilteil wird die Aktivierung oder Deaktivierung erst wirksam, wenn es aus- und wieder eingeschaltet wird. Im Modus **Deaktiv** wirkt die Echounterdrückung nicht und es können bei VoIP-Verbindungen über DECT-Mobilteile Echos auftreten. Standard: Deaktiv
Economic Mode	
Economic Mode	Der ECO Mode kann für alle DECT-Telefone systemweit aktiviert werden. Dabei wird die Sendeleistung der DECT-Telefone entweder um einen fest eingestellten Wert gesenkt (statisch) oder jedes DECT-Telefon passt seine Sendeleistung selbstständig an die empfangene Signalstärke an (adaptiv). Standard: Deaktiv
Economic Mode: **Aus**	Der ECO Mode ist systemweit deaktiviert.
Economic Mode: **Ein**	Der ECO Mode (statisch) ist systemweit aktiviert. Die Sendeleistung der DECT-Telefone wird um einen festen Wert gesenkt.
Economic Mode: **Adaptiv**	Der ECO Mode (adaptiv) ist systemweit aktiviert. Jedes einzelne DECT-Telefone passt seine Sendeleistung selbstständig an die empfangene Signalstärke an. Bei Handover wird zuerst auf die hohe Sendeleistung geschaltet und anschließend abhängig vom Empfang die Sendeleistung reduziert.

27.3.8.2 Cordless > SLC

Parameterbeschreibung der Registerkarten:

- **DECT Teilnehmer ändern**

Parameter	Beschreibung
Rufnr	Rufnummer des DECT-Telefons.
DuWa	Durchwahlnummer des DECT-Telefons.
Name	Namens des DECT-Telefons.
Aktiv	Anmeldestatus des DECT-Telefons: Grün: DECT-Telefon ist aktiv. Rot: Baugruppen-Sperrschalter bei angemeldetem DECT-Telefon gesetzt. Gelb: DECT-Telefon wurde durch Änderung der PIN automatisch wieder abgemeldet. Grau: An diesem Port wurde noch nie ein DECT-Telefon angemeldet.

Parameter	Beschreibung
Mobilcode	PIN-Code zur Anmeldung des DECT-Telefons. Der Mobilcode muss systemweit eindeutig sein.
Access	Name, Nummer und Einbauplatz der S_0-Verlängerungsleitung.
Slot	Anzeige des Slots der gesteckten SLC-Baugruppe.
Schaltflächen	
Löschen	Das DECT-Telefon wird im System ausgetragen. Dabei werden Rufnummer, Durchwahl und Name gelöscht und die zugehörige TDM User Lizenz freigegeben.

Parameterbeschreibung der Registerkarten:

- **DECT Teilnehmer hinzufügen**

Parameter	Beschreibung
Systemkennung	Gehört das Kommunikationssystem nicht zu einem Netzverbund (Knoten-ID = 0), wird die Systemkennung mit 1 vorbelegt. Gehört das Kommunikationssystem zu einem Netzverbund (Knoten-ID > 0), muss die Systemkennung mit der Knoten-ID übereinstimmen (**Cordless > Multi SLC > Systemkennung**).
Slot	Slot der gesteckten SLC-Baugruppe.
SLC-Nr.	Systemweit eindeutige ID-Nummer der SLC- Baugruppe. Wertebereich: 1-15,17-31,33-47,...,127. Vielfache von 16 sind nicht erlaubt.
Anzahl DECT-Telefone	Anzahl der bereits konfigurierten DECT-Telefone diese SLC-Baugruppe.
SLC Rufnummer	Systemweit eindeutige Rufnummer der S_0-Verlängerungsleitung.
Access	Name, Nummer und Einbauplatz der S_0-Verlängerungsleitung.
DECT-Teilnehmer hinzufügen	
Anzahl DECT-Telefone	Ist die Anzahl der DECT-Telefone kleiner als die im System zulässige Größe (Versionsabhängig), lässt sich hier eine zusätzliche Anzahl von DECT-Telefonen für diese SLC-Baugruppe hinzufügen. Die neu hinzugefügten DECT-Telefone werden unter der Registerkarte **DECT Teilnehmer ändern** angezeigt.

27.3.8.3 Cordless > Multi-SLC

Parameterbeschreibung der Registerkarten:

- **Multi-SLC ändern**

Parameter	Beschreibung
SLC-Nr.	Systemweit eindeutige ID-Nummer der SLC- Baugruppe. Wertebereich: 1-15,17-31,33-47,...,127. Vielfache von 16 sind nicht erlaubt.
Knoten-ID	Anzeige der Knoten-ID (falls konfiguriert). Gehört das Kommunikationssystem zu einem Netzverbund, werden hier alle konfigurierten SLC-Baugruppen des Netzverbundes angezeigt.
SLC Rufnummer	Systemweit eindeutige Rufnummer der S_0-Verlängerungsleitung der SLC- Baugruppe.

27.3.8.4 Cordless > Basisstationen

Parameterbeschreibung der Registerkarten:

- **Basisstation ändern**

Parameter	Beschreibung
Slot	Anzeige des Slots, in dem die SLC-Baugruppe der Basisstation gesteckt ist. Für das Mainboard (SLUC) wird Slot 2 angezeigt.
Typ	Typ der Basisstation. Bei einer SLC-Baugruppe wird der Typ nur angezeigt, bei SLUC kann der Typ ausgewählt werden. Wenn der Typ von **Kein Port** auf **Basisstation** geändert wird, werden automatisch 16 DECT-Telefone vorkonfiguriert und eine SLC-Vernetzungsleitung eingerichtet.
Typ: **Basisstation**	Basisstation angeschaltet.
Typ: **Kein Port**	keine Basisstation angeschaltet.
Name	Name der Basisstation.
Pegel	Pegel der Basisstation. Wertebereich: 50% und 100%, Standardwert: 100%
Status	Status der Basisstation.
Masterport	Bei einer SLC-Baugruppe werden die Ports angezeigt, an denen die Basisstationen angeschaltet sind. Bei SLUC werden alle Ports mit den angeschlossenen Endgeräten angezeigt.

27.3.9 Kommende Rufe

Unter **Kommende Rufe** sind die Funktionen für das sogenannte Call Management (CM) zusammengefasst. Dazu gehören z. B. Einstellungen für Gruppen und die Rufweiterschaltung.

27.3.9.1 Kommende Rufe > Gruppen-/Sammelanschluss

Für die Erstkonfiguration von Gruppenrufen und Sammelanschlüssen wird empfohlen, den Wizard **Gruppenruf / Sammelanschluss** zu verwenden.

Parameterbeschreibung der Registerkarten:

- **Gruppenrufnummern bearbeiten**
- **Verwendete Gruppen anzeigen**
- **Alle Gruppenmitglieder anzeigen**
- **Gruppe hinzufügen**
- **Gruppe löschen**
- **Gruppenparameter ändern**
- **Mitglieder anzeigen**
- **Mitglied hinzufügen**
- **Mitglieder-Reihenfolge ändern**
- **Basic-MULAP-Überlappung prüfen**
- **MULAP-Präferenz prüfen**

Parameter	Beschreibung
Index	Fortlaufende Nummer, die vom Kommunikationssystem vergeben wird.
Ruf-Nr. **Rufnummer**	Rufnummer des Gruppenrufs, des Sammelanschlusses, der Basic-MULAP, der Chef-MULAP oder der Sprachbox-Gruppe
DuWa **Durchwahlnummer**	Durchwahlnummer des Gruppenrufs, des Sammelanschlusses, der Basic-MULAP, der Chef-MULAP oder der Sprachbox-Gruppe
Name	Name des Gruppenrufs, des Sammelanschlusses, der Basic-MULAP, der Chef-MULAP oder der Sprachbox-Gruppe
Typ	Definition des Gruppentyps Standardwert: Gruppe
Typ: Linearer Sammelanschluss	Ein ankommender Anruf wird immer zuerst beim ersten Mitglied des Sammelanschlusses signalisiert. Die weitere Signalisierung erfolgt anhand der in der Gruppentabelle eingetragenen Reihenfolge der Mitglieder.
Typ: Zyklischer Sammelanschluss	Ein ankommender Anruf wird zuerst bei dem Mitglied signalisiert, der dem Teilnehmer nachfolgt, der den letzten Anruf angenommen hat. Die weitere Signalisierung erfolgt anhand der in der Gruppentabelle eingetragenen Reihenfolge der Mitglieder.
Typ: Gruppe	Gruppenruf des Typs Gruppe: Ankommende Anrufe werden gleichzeitig bei allen verfügbaren Gruppenmitgliedern signalisiert. Verfügbare Gruppenmitglieder sind Teilnehmer, die nicht besetzt sind. Sind alle Gruppenmitglieder besetzt, wird ein Anruf durch einen Anklopfton signalisiert. Legt ein Teilnehmer auf, wird der Anruf weiterhin bei allen Gruppenmitgliedern signalisiert (Anklopfton bei besetzten Gruppenmitgliedern).
Typ: Freifall	Gruppenruf des Typs Freifall: Ankommende Anrufe werden gleichzeitig bei allen Gruppenmitgliedern signalisiert. Ist ein Mitglied der Gruppe besetzt, wird der gesamte Gruppenruf als besetzt gekennzeichnet. Weitere Anrufer erhalten den Besetztton.

Parameter	Beschreibung
Typ: Basic-MULAP	Ankommende Anrufe werden bei allen zur Basic-MULAP (MULAP = Multiple Line Appearance) gehörenden Telefonen optisch signalisiert. Für jedes Mitglied kann zusätzlich angegeben werden, ob ankommende Anrufe auch akustisch signalisiert werden sollen. Nach Annahme des Anrufs ist die Basic-MULAP besetzt und weitere Anrufer erhalten den Besetztton. Bei gehenden Anrufen über die Basic-MULAP-Leitung wird den Angerufenen die Basic-MULAP-Rufnummer im Display angezeigt.
Typ: Chef-MULAP	Chef-MULAPs können eingerichtet werden, wenn eingeschränkte Chef- und Sekretär-Funktionen genutzt werden sollen. Wählt ein Anrufer die Chef-MULAP-Rufnummer, wird der Anruf bei allen zur Chef- MULAP gehörenden Telefonen optisch signalisiert. Bei Mitgliedern mit Sekretär-Funktionen werden ankommende Anrufe auch akustisch signalisiert.
Typ: Anklopfen	Gruppenruf des Typs Anklopfen: Ankommende Anrufe werden gleichzeitig bei allen verfügbaren Gruppenmitgliedern signalisiert. Verfügbare Gruppenmitglieder sind Teilnehmer, die nicht besetzt sind. Bei besetzten Gruppenmitgliedern wird ein anstehender Anruf sofort durch einen Anklopfton signalisiert.
Typ: Anrufbeantworter	Sprachbox-Gruppe: Durch eine Sprachbox-Gruppe (Anrufbeantworter-Gruppe) kann einer bestimmten Gruppe von Teilnehmern der Zugriff auf Sprachnachrichten ermöglicht werden. Über die Rufnummer der Sprachbox-Gruppe werden nicht die Mitglieder dieser Gruppe gerufen, sondern wird direkt die Sprachbox (der Anrufbeantworter) der Gruppe erreicht. Nachdem eine Sprachnachricht auf der Sprachbox der Gruppe hinterlassen wurde, erfolgt eine Weiterleitung an die Sprachboxen aller Mitglieder. Alle Mitglieder erhalten die Sprachnachricht gleichzeitig. Löscht ein Mitglied der Gruppe eine Sprachnachricht, wird diese auch aus den Sprachboxen aller anderen Mitglieder und aus der Sprachbox der Gruppe gelöscht. Die persönlichen Sprachnachrichten aller Mitglieder bleiben davon unbeeinflusst.
Rufart	Definition der akustischen Signalisierung kommender externer Anrufe der Gruppe Standardwert: 1 Bei analogen Telefonen ist ausschließlich die Standardeinstellung möglich. Änderungen haben keine Auswirkung.
Rufart: 1	Doppel-Rufton
Rufart: 2	Dreifach-Rufton
Rufart: 3	Kurz/Lang/Kurz-Rufton
Tel.-Buch	Bei aktiviertem Flag (Anzeige Ja) erscheint die Rufnummer der Gruppe im internen Verzeichnis. Standardwert: Aktiviert
Gruppenmitglied	
Gruppe	Nummer (Index) der Gruppe
Mitglied	Nummer (Index) des Mitglieds innerhalb der Gruppe
Rufnummer	Rufnummer des Gruppenmitglieds
Name	Name des Gruppenmitglieds
Parameter	Aktivierte Parameter des Gruppenmitglieds

Parameter	Beschreibung
Parameter: M	Master (M): Basic-MULAP: Das Mitglied ist Master der Basic-MULAP. Chef-MULAP: Das Mitglied hat Chef-Funktionen.
Parameter: R	Akustischer Ruf (R): Basic-MULAP und Chef-MULAP: Ankommende Anrufe werden akustisch signalisiert.
Parameter: A	Automatische Belegung gehend (A): Basic-MULAP: Beim Abheben des Hörers wird automatisch über die Basic-MULAP-Leitung gerufen. Chef-MULAP: Beim Abheben des Hörers wird automatisch über die Chef-MULAP-Leitung gerufen.
Parameter: K	Keine automatische Rufannahme kommend (K): Basic-MULAP und Chef-MULAP: Ein kommender Anruf muss durch Betätigen der MULAP-Taste angenommen werden.
Parameter: P	Automatische Konferenz Freigabe (P): Basic-MULAP und Chef-MULAP: Durch Drücken der MULAP-Taste wird die belegte MULAP-Leitung für eine Konferenz freigegeben.
MULAP-Taste eingerichtet	Angezeigt wird, ob für das Gruppenmitglied eine MULAP-Taste eingerichtet wurde oder nicht.
Richtung	Bei einem externen Gruppenmitglied wird die Richtung angezeigt.
Gruppe	
Konsistenz Check	Angezeigt werden eventuelle Kollisionen durch Überlappung bei Mastern von Basic-MULAPs oder bei der automatischen Belegung gehend von Basic-MULAPs.

27.3.9.2 Kommende Rufe > Gruppen-Teilnehmer

Parameterbeschreibung der Registerkarten:

- **Mitglied ändern**
- **Mitglied löschen**

Parameter	Beschreibung
Gruppe	Nummer (Index) der Gruppe
Gruppenmitglied	Nummer (Index) des Gruppenmitglieds
Rufnummer	Rufnummer des Gruppenmitglieds
Name	Name des Gruppenmitglieds
MULAP-Name	Name der MULAP (Multiple Line Appearance)-Gruppe
MULAP-Ruf-Nr.	Rufnummer der MULAP-Gruppe

Parameter	Beschreibung
Master (M)	Basic-MULAP: Durch Aktivierung dieses Flags wird ein Mitglied zu einem Master der Basic-MULAP. Aktiviert ein Master eine Anrufumleitung, gilt diese für alle Mitglieder (Telefone) der Basic-MULAP. Chef-MULAP: Durch Aktivierung dieses Flags werden einem Mitglied Chef-Funktionen zugewiesen. Beim Abheben des Hörers wird automatisch über die Chef-MULAP-Leitung gerufen. Ankommende Anrufe über Chef-MULAP-Rufnummer werden ausschließlich optisch signalisiert.
Akustischer Ruf (R)	Basic-MULAP und Chef-MULAP: Bei aktiviertem Flag werden ankommende Anrufe akustisch signalisiert. Standardwert: Aktiviert für alle Master einer Basic-MULAP. Aktiviert für alle Mitglieder mit Sekretär-Funktion einer Chef-MULAP.
Automatische Belegung gehend (A)	Basic-MULAP: Bei aktiviertem Flag wird beim Abheben des Hörers automatisch über die Basic-MULAP-Leitung gerufen. Chef-MULAP: Bei aktiviertem Flag wird beim Abheben des Hörers automatisch über die Chef-MULAP-Leitung gerufen. Standardwert: Aktiviert für alle Master einer Basic-MULAP. Aktiviert für alle Mitglieder mit Chef-Funktion einer Chef-MULAP.
Keine automatische Rufannahme kommend (K)	Basic-MULAP und Chef-MULAP: Bei aktiviertem Flag kann ein kommender Anruf nicht durch Abheben des Hörers angenommen werden. Die Annahme eines kommenden Anrufs ist ausschließlich durch Betätigen der MULAP-Taste möglich. Standardwert: Deaktiviert
Automatische Konferenz Freigabe (P)	Basic-MULAP und Chef-MULAP: Bei aktiviertem Flag wird durch Drücken der MULAP-Taste die belegte MULAP-Leitung für eine Konferenz freigegeben. Bei allen weiteren Mitgliedern wird die Freigabe durch Blinken der MULAP-Taste angezeigt. Durch das Drücken der MULAP-Taste können sie sich in die Konferenz hineinschalten. Standardwert: Deaktiviert
MULAP-Taste eingerichtet	Basic-MULAP: Bei aktiviertem Flag wird bei dem zugehörigen Telefon eine MULAP-Taste eingerichtet. Durch Drücken der Taste erfolgt eine gehende Belegung über die Basic-MULAP-Leitung. Dem Angerufenen wird die Basic-MULAP-Rufnummer im Display angezeigt. Chef-MULAP: Bei aktiviertem Flag wird bei dem zugehörigen Telefon eine MULAP-Taste eingerichtet. Durch Drücken der Taste erfolgt eine gehende Belegung über die Chef-MULAP-Leitung. Dem Angerufenen wird die Chef-MULAP-Rufnummer im Display angezeigt. Standardwert: Aktiviert
Richtung	Bei einem externen Gruppenmitglied wird die Richtung angezeigt.
Typ	Definition des Gruppentyps

27.3.9.3 Kommende Rufe > Team/Top

Für die Erstkonfiguration von Team- und Top-Gruppen wird empfohlen, die Wizards **Teamschaltung** und **Chef / Sekretär** zu verwenden.

Parameterbeschreibung der Registerkarten:

- **Alle Team/Top Gruppen anzeigen**
- **Verwendete Team/Top Gruppen anzeigen**
- **Team/Top Gruppe hinzufügen**
- **Team/Top Gruppe ändern**
- **Team/Top Gruppe löschen**
- **Team/Top Gruppen-Parameter ändern**
- **Alle Team/Top Gruppen-Mitglieder anzeigen**
- **Team/Top Mitglied hinzufügen**
- **Team/Top Mitglied ändern**
- **Team/Top Mitglied löschen**
- **Fax Boxen anzeigen**
- **Fax Box hinzufügen**

Parameter	Beschreibung
Index	Fortlaufende Nummer, die vom Kommunikationssystem vergeben wird.
Name	Name der Team/Top-Gruppe
Art	Definition des Gruppentyps
Art: Team	Eine Team-Gruppe bietet komfortable Funktionen für Teams. Die Rufnummern aller Teammitglieder werden auf MULAP-Tasten (Leitungstasten) programmiert. Damit hat jedes Teammitglied Zugriff auf alle Leitungen (zum Beispiel zur Anrufübernahme) und kann auch gleichzeitig über mehrere Leitungen telefonieren.
Art: Top	Eine Top-Gruppe bietet komfortable Chef- und Sekretär-Funktionen (Topfunktion) für bis zu drei Chefs und bis zu drei Sekretäre.
Tastenvergabe auf Team	Definition für die Einrichtung der MULAP-Tasten des Mitglieds der Team-Gruppe
Tastenvergabe auf Team: auf erste/zweite Konsole	Bei aktiviertem Flag erfolgt eine automatische Einrichtung der MULAP-Tasten auf dem ersten oder zweiten Beistellgerät (Key Module oder BLF) des Team-Telefons.
Tastenvergabe auf Team: auf erste freie Tasten	Bei aktiviertem Flag erfolgt eine automatische Einrichtung der MULAP-Tasten auf den ersten freien Tasten des Team-Telefons.
Tastenvergabe auf Top	Definition für die Einrichtung der MULAP-Tasten des Mitglieds der Top-Gruppe
Tastenvergabe auf Top: auf erste/zweite Konsole	Bei aktiviertem Flag erfolgt eine automatische Einrichtung der MULAP-Tasten auf dem ersten oder zweiten Beistellgerät (Key Module oder BLF) des Top-Telefons.
Tastenvergabe auf Top: auf erste freie Tasten	Bei aktiviertem Flag erfolgt eine automatische Einrichtung der MULAP-Tasten auf den ersten freien Tasten des Top-Telefons.
Gruppenmitglied	
Gruppe	Nummer (Index) der Gruppe
Mitglieder	Nummer (Index) des Mitglieds innerhalb der Gruppe
Typ	Definition des Mitgliedstyps
Ruf-Nr.	Rufnummer des Gruppenmitglieds (Ändert sich in einer MULAP-Gruppe in **Rufnr. und ist intern unter dieser **Rufnr. erreichbar.)
Name	Name des Gruppenmitglieds
MULAP-Ruf-Nr.	Rufnummer der MULAP-Gruppe

Parameter	Beschreibung
MULAP-Duwa	Durchwahlnummer der MULAP-Gruppe
MULAP-Name	Name der MULAP-Gruppe
Rufart	Definition der akustischen Signalisierung kommender externer Anrufe der Gruppe Standardwert: 1 Bei analogen Telefonen ist ausschließlich die Standardeinstellung möglich. Änderungen haben keine Auswirkung.
Rufart: 1	Doppel-Rufton
Rufart: 2	Dreifach-Rufton
Rufart: 3	Kurz/Lang/Kurz-Rufton
Tel.-Buch	Bei aktiviertem Flag (Anzeige Ja) erscheint die Rufnummer der Gruppe im internen Verzeichnis. Standardwert: Aktiviert
Master (M)	Team-Gruppe: Durch Aktivierung dieses Flags wird ein Mitglied zu einem Master der Team-Gruppe. Aktiviert ein Master eine Anrufumleitung, gilt diese für alle Mitglieder (Telefone) der Team-Gruppe. Top-Gruppe: Durch Aktivierung dieses Flags erhält ein Mitglied Chef-Funktionen. Beim Abheben des Hörers wird automatisch über die MULAP-Leitung dieses Mitglieds gerufen. Ankommende Anrufe über die zugehörige Chef-MULAP-Rufnummer werden standardmäßig ausschließlich optisch signalisiert.
Akustischer Ruf (R)	Team-Gruppe und Top-Gruppe: Bei aktiviertem Flag werden ankommende Anrufe akustisch signalisiert. Standardwert: Aktiviert für alle Mitglieder einer Team-Gruppe. Aktiviert für alle Mitglieder mit Sekretär-Funktion einer Top-Gruppe.
Automatische Belegung gehend (A)	Team-Gruppe und Top-Gruppe: Bei aktiviertem Flag wird beim Abheben des Hörers automatisch über die MULAP-Leitung dieses Mitglieds gerufen. Standardwert: Aktiviert
Keine automatische Rufannahme kommend (K)	Team-Gruppe und Top-Gruppe: Bei aktiviertem Flag kann ein kommender Anruf nicht durch Abheben des Hörers angenommen werden. Die Annahme eines kommenden Anrufs ist ausschließlich durch Betätigen der MULAP-Taste möglich. Standardwert: Deaktiviert
Automatische Konferenz Freigabe (P)	Team-Gruppe und Top-Gruppe: Bei aktiviertem Flag wird durch Drücken der MULAP-Taste die belegte MULAP-Leitung für eine Konferenz freigegeben. Bei allen weiteren Mitgliedern wird die Freigabe durch Blinken der MULAP-Taste angezeigt. Durch das Drücken der MULAP-Taste können sie sich in die Konferenz hineinschalten. Standardwert: Deaktiviert

Parameter	Beschreibung
MULAP-Taste eingerichtet	Team-Gruppe: Bei aktiviertem Flag wird bei dem zugehörigen Telefon eine MULAP-Taste eingerichtet. Durch Drücken der Taste erfolgt eine gehende Belegung über die MULAP-Leitung des Masters. Dem Angerufenen wird die MULAP-Rufnummer des Masters im Display angezeigt. Top-Gruppe: Bei aktiviertem Flag wird bei dem zugehörigen Telefon eine MULAP-Taste eingerichtet. Durch Drücken der Taste erfolgt eine gehende Belegung über die Chef-MULAP-Leitung. Dem Angerufenen wird die Chef-MULAP-Rufnummer im Display angezeigt. Standardwert: Deaktiviert für alle Mitglieder einer Team-Gruppe. Aktiviert für alle Mitglieder einer Top-Gruppe.
MULAP Typ	Definition des MULAP-Typs
MULAP Typ: Basic-MULAP	Ankommende Anrufe werden bei allen zur Basic-MULAP gehörenden Telefonen optisch signalisiert. Für jedes Mitglied kann zusätzlich angegeben werden, ob ankommende Anrufe auch akustisch signalisiert werden sollen. Nach Annahme des Anrufs ist die Basic-MULAP besetzt und weitere Anrufer erhalten den Besetztton. Bei gehenden Anrufen über die Basic-MULAP-Leitung wird den Angerufenen die Basic-MULAP-Rufnummer im Display angezeigt.
MULAP Typ: Chef-MULAP	Alle Mitglieder einer Chef-MULAP sind unter der Chef-MULAP-Rufnummer und unter ihren eigenen Teilnehmerrufnummern erreichbar.
Fax Ruf-Nr.	Rufnummer der Faxbox des Gruppen-Mitglieds
Fax DuWa	Durchwahlnummer der Faxbox des Gruppen-Mitglieds

27.3.9.4 Kommende Rufe > Anrufübernahme

Parameterbeschreibung der Registerkarten:

- **Namen Anrufübernahmegruppen ändern**
- **Teilnehmer der Gruppe anzeigen**
- **Teilnehmer der Gruppe zuordnen**

Parameter	Beschreibung
Gruppe	
Gruppe	Nummer (Index) der Anrufübernahmegruppe Wertebereich: 1 bis 32
Name	Name der Anrufübernahmegruppe
Teilnehmer	
Ruf-Nr.	Rufnummer des internen Teilnehmers
Name	Name des internen Teilnehmers
Zuordnung Gruppe X	Bei aktiviertem Flag ist der Teilnehmer der Anrufübernahmegruppe X zugeordnet.
Gruppe	Anrufübernahmegruppe, der dieser Teilnehmer zugeordnet ist.

27.3.9.5 Kommende Rufe > UCD

Parameterbeschreibung der Registerkarte:

- **UCD Parameter ändern**

Parameter	Beschreibung
UCD-Flags	
UCD-Applikation freigeben	Bei aktiviertem Flag ist das Leistungsmerkmal Anrufverteilung (Uniform Call Distribution UCD) systemweit freigegeben. Standardwert: Aktiviert
Agenten dauerverfügbar	Bei aktiviertem Flag sind alle UCD-Agenten dauerverfügbare Agenten. Ein dauerverfügbarer Agent bleibt auch dann für Anrufe, Faxe und E-Mails verfügbar, wenn er einen Anruf, ein Fax oder eine E-Mail nicht angenommen hat. Standardwert: Deaktiviert
Automatische Nachbearbeitungszeit	
Nachbearbeitungszeit (Zyklen)	Systemweite Definition der automatischen Nachbearbeitungszeit für alle UCD-Agenten in Rufzyklen, das heißt in 5-Sekunden-Schritten. Während der Nachbearbeitungszeit wird ein Agent kurzzeitig von der Anrufverteilung ausgenommen, um Nacharbeiten für den soeben beendeten Anruf durchführen zu können. Standardwert: 0
Priorität bei internen Rufen	
Priorität intern	Systemweite Definition der Priorität für interne Anrufe anhand von 10 Prioritätsebenen (1 = hoch, 10 = niedrig). Standardwert: 10
Priorität bei externen Rufen	
Slot/Leitung	Anzeige der Baugruppe, des Einbauplatzes (Slot) und der Nummer der Leitung (des B-Kanals). Für externe Anrufe erfolgt die Prioritätsvergabe leitungsbezogen (pro B-Kanal), unabhängig davon, ob es sich um IP- oder TDM-Leitungen handelt.
Priorität	Definition der Priorität für externe Anrufe, die über die betreffende Leitung (B-Kanal) eingehen. Die Definition erfolgt anhand von 10 Prioritätsebenen (1 = hoch, 10 = niedrig). Standardwert: 1

Parameterbeschreibung der Registerkarten:

- **UCD Gruppen anzeigen**
- **UCD Gruppe ändern**

Parameter	Beschreibung
Rufnummer	Rufnummer der UCD-Gruppe
Durchwahlnummer	Durchwahlnummer der UCD-Gruppe
Name	Name der UCD-Gruppe

Parameter	Beschreibung
Prim. Rufzykl.	Definition des primären Rufzyklus: Die Definition erfolgt in Rufzyklen, das heißt in 5-Sekunden-Schritten. Eingestellt wird die Zeit, die ein Anruf in der Warteschlange verbleibt, falls er nicht von dem am längsten im Zustand verfügbar befindlichen Agenten angenommen wird. Anschließend wird der Anruf zum nächsten verfügbaren Agenten weitergegeben. Standardwert: 3 Zyklen
Sek. Rufzykl.	Definition des sekundären Rufzyklus: Die Definition erfolgt in Rufzyklen, das heißt in 5-Sekunden-Schritten. Eingestellt wird die Zeit, die ein Anruf in der Warteschlange verbleibt, falls er nicht von dem nächsten verfügbaren Agenten angenommen wird. Standardwert: 3 Zyklen
Wart. Anrufe	Definition der maximalen Anzahl wartender Anrufe: Die über diese Anzahl hinausgehenden Anrufe können an ein Überlaufziel (ein externes Ziel, eine andere UCD-Gruppe, ein interner Teilnehmer oder eine Gruppe) weitergeleitet werden. Standardwert: 10 (Standardwert letzte UCD-Gruppe: 72)
AICC	Definition der Automatic Incoming Call Connection AICC. Die Einstellung gilt für alle Agenten einer UCD-Gruppe, unabhängig davon, ob das Telefon eines Agenten mit Headset ausgestattet ist oder nicht. Standardwert: Nein
AICC: ja	Die Agenten dieser UCD-Gruppe können kommende Anrufe ohne zusätzliche Bedienschritte annehmen. Der Agent wird durch einen Hörton im Headset auf das Eintreffen eines Anrufes aufmerksam gemacht, der anschließend automatisch durchgeschaltet wird.
AICC: nein	Die Agenten dieser UCD-Gruppe können kommende Anrufe nicht ohne die herkömmlichen Bedienschritte (zum Beispiel durch das Abnehmen des Hörers) annehmen.
Ansagewechsel	Definition möglicher Ansagewechsel Standardwert: Einmalig
Ansagewechsel: Einmalig	Die in der Warteschlange befindlichen Anrufer erhalten eine einmalige Ansage.
Ansagewechsel: Zyklisch	Die in der Warteschlange befindlichen Anrufer erhalten zyklisch wechselnde Ansagen.
Overflow-Zeit	Definition der Overflow-Zeit in Sekunden: Wird ein wartender Anruf nicht innerhalb der Overflow-Zeit durch die UCD-Applikation angenommen, wird der Anruf anhand der Angaben im Call Management durch das Kommunikationssystem weiterverarbeitet. Diese Einstellung ist ausschließlich relevant, wenn eine externe UCD-Applikation angeschlossen ist. Standardwert: 600
Ansageverzögerung	Definition der Ansageverzögerung in Sekunden: Nach Ablauf dieser Zeit erhält ein Anrufer in der Warteschlange eine Ansage. Standardwert: 0

Parameterbeschreibung der Registerkarte:

- **UCD Gruppen Parameter ändern**

Parameter	Beschreibung
Ziel-Index	Für jede UCD-Gruppe können bis zu sieben Ziele (Index 1 bis 7) für Wartemusik (Music On Hold MOH) oder Ansagen definiert werden, die nacheinander eingespielt werden.
Ansageeinrichtungen	Wartemusik oder Ansage für den betreffenden Ziel-Index
Wartezeit	Definition der Wartezeit: Nach Ablauf dieser Zeit wird einem Anrufer in der Warteschlange die nächste Wartemusik oder Ansage eingespielt. Die Definition erfolgt in Rufzyklen, das heißt in 5-Sekunden-Schritten. Standardwert: 1 Zyklus

Parameterbeschreibung der Registerkarte:

- **UCD Gruppen Mitglied hinzufügen/löschen**

Parameter	Beschreibung
Auswahl	Liste aller UCD-Agenten-IDs. Die UCD-Agenten-IDs entsprechen nicht den Rufnummern im Kommunikationssystem.
Mitglieder	Liste der UCD-Agenten-IDs der gewählten UCD-Gruppe
Schaltflächen	
Hinzufügen	Fügt die markierten UCD-Agenten-IDs der UCD-Gruppe hinzu.
Löschen	Löscht die markierten UCD-Agenten-IDs aus der UCD-Gruppe.

Parameterbeschreibung der Registerkarte:

- **Teilnehmer zuweisen**

Parameter	Beschreibung
Agenten-ID	Liste der UCD-Agenten-IDs der gewählten UCD-Gruppe.
Teilnehmer	Liste der Teilnehmer, die den UCD-Agenten-IDs der UCD-Gruppe zugeordnet werden können.

27.3.9.6 Kommende Rufe > Rufweiterschaltungen

Parameterbeschreibung der Registerkarten:

- **Rufzielliste - Definition**

Parameter	Beschreibung
Rufzielliste	Auswahl der zu bearbeitenden Rufzielliste. Wertebereich: 1 bis 740
Rufweiterschaltung ändern Um ein Rufziel schneller zu finden, können Sie in den Feldern **1. - 4. Ziel** auch eine oder mehrere Ziffern eingeben. Dann wird direkt zum Listeneintrag gesprungen, der mit der eingegebenen Ziffernfolge beginnt. Die Eingabe einer Buchstabenfolge ist ebenfalls möglich.	
1. - 4. Ziel: **kein Eintrag**	Rufziel wird übersprungen.

Parameter	Beschreibung
1. - 4. Ziel: **externes Ziel**	Richtung und externe Rufnummer mit Amtskennzahl.
1. - 4. Ziel: *** Angewählter Teilnehmer**	Angerufener Teilnehmer.
1. - 4. Ziel: **** Benutzer definiert**	Ziel der Anrufumleitung nach Zeit (falls eingerichtet).
1. - 4. Ziel: **#9 Systemsuchlauf**	Nächster verfügbarer Teilnehmer (außer Chef-Nebenstelle).
1. - 4. Ziel: **#201 - #260**	Anrufverteilung (UCD-Gruppe).
1. - 4. Ziel: **#801 - #817**	Ansagegerät.
1. - 4. Ziel: 100, 101, ...	Rufnummer eines Teilnehmers oder einer Gruppe (z. B. Sprachbox)
Die Rufweiterschaltung erfolgt immer nach	Zeit, nach der ein Anruf an das nächste Rufziel weitergeschaltet wird. Bei UCD-Gruppen folgt die Weiterschaltung den Mechanismen der primären und sekundären Rufzyklen (siehe UCD-Gruppen). Wertebereich: 5/10/15/...75 s, Standardwert: 15 s
Rufweiterschaltung	Anruf wird im Besetztfall sofort an das nächste Rufziel weitergeleitet. Standardwert: aktiviert
Zweitwecker	
Zweitwecker Ziel	Zusätzlicher interner Teilnehmer, bei dem der Anruf ebenfalls signalisiert wird oder ein Aktor (Relais) einer Aktoren/Sensoren-Baugruppe für einen zentralen Wecker.
Zweitwecker Art	Der Anruf kann sofort oder nach der gesamten Rufweiterschaltungszeit beim Teilnehmer signalisiert werden. Standardwert: Sofort

Parameterbeschreibung der Registerkarten:

- **Rufzielliste - Zuordnung**

Parameter	Beschreibung
Rufnr	Rufnummer des Teilnehmers bzw. der Gruppe.
Name	Name des Teilnehmers bzw. der Gruppe.
Art	Teilnehmer-Typ, z. B. U_{P0}, System-Client, AB, ISDN, SIP.
Tag	Nummer der Rufzielliste, für kommende Externrufe während der Arbeitszeiten (Tagschaltung) Standardwert: 14

Parameter	Beschreibung
Nacht	Nummer der Rufzielliste für kommende Externrufe bei aktivierter Nachtschaltung Standardwert: 15
Intern	Nummer der Rufzielliste für kommende Internrufe Standardwert: 16
Suche	Wird in die Suchfelder **Rufnr** oder **Name** ein Suchbegriff eingegeben und anschließend die Return-Taste gedrückt, werden alle Treffer angezeigt, die den Suchbegriff enthalten. Mit der Eingabe von `521` als Rufnummer werden z. B. die Treffer `+495213535` und `+498967521` angezeigt oder mit `co` als Name die Treffer `Collins`, `Mcoin` und `Branco`. Alle Einträge werden angezeigt, wenn in allen Suchfeldern nichts eingetragen ist und anschließend die Return-Taste gedrückt wird.

Parameterbeschreibung der Registerkarten:

- **Rufziellisten-Teilnehmer**

Parameter	Beschreibung
Alle Teilnehmer in Rufzielliste anzeigen	Für die ausgewählte Rufzielliste werden alle Teilnehmer bzw. Gruppen angezeigt, die diese Rufzielliste nutzen.

Parameterbeschreibung der Registerkarten:

- **Rufziellisten zuweisen**

Parameter	Beschreibung
Rufzielliste	Auswahl der Rufzielliste, der Teilnehmer zugewiesen werden sollen. Wertebereich: 1 bis 740
Tag	Rufzielliste ist für kommende Externrufe während der Arbeitszeiten (Tagschaltung)
Nacht	Rufzielliste ist für kommende Externrufe bei aktivierter Nachtschaltung
Intern	Rufzielliste ist für kommende Internrufe
Rufziellisten	
Auswahl	Liste aller Teilnehmer.
Mitglieder	Liste der Teilnehmer, denen die Rufzielliste zugeordnet ist.
Schaltflächen	
Hinzufügen	Markierte Teilnehmer werden aus dem Auswahl-Fenster in das Mitglieder-Fenster übernommen.
Löschen	Markierte Teilnehmer werden aus dem Mitglieder-Fenster gelöscht.

27.3.10 Leitungen/Vernetzung

Unter **Leitungen/Vernetzung** sind die Funktionen für die Amtsleitungen und die Richtungen zusammengefasst.

27.3.10.1 Leitungen/Vernetzung > Leitungen

Parameterbeschreibung der Registerkarten:

- **Alle Leitungen anzeigen**
- **Richtung ändern**

Parameter	Beschreibung
Leitung	Anzeige der an das Kommunikationssystem angeschlossenen physikalischen Amtsleitung.
Box-Sl-Pt-Le oder Box/Slot/Port/Leitung	Anzeige des Baugruppentyps sowie die Einbauplatz- und Port-Nummer (physikalischen Port) für den Anschluss der Leitung an das Kommunikationssystem.
Kennzahl	Anzeige oder Einrichtung der Richtungskennzahl. Bei Eingabe dieser Nummer wird vom Kommunikationssystem die zugeordnete Leitung belegt. Diese dient zum Prüfen einer Leitung oder zur Programmierung einer Leitungstaste.
Richtung	Anzeige oder Auswahl der Richtung, die der Leitung zugeordnet ist (keine oder Rtg.1 bis Rtg.12). Wird für eine aktive Leitung die Auswahl „keine“ eingestellt, verhält sich das System unstabil. Außerdem kann das System zwar auf dieser Leitung einen Anruf empfangen, aber der Anruf kann nicht weitergeleitet werden.
Status	Anzeige des Leitungszustands. Eine inaktive Leitung wird durch einen Stern gekennzeichnet.
Typ	Anzeige des Leitungstyps. Inaktive Leitungen erhalten die Bezeichnung “No Port”.

Parameterbeschreibung der Registerkarten:

- **Rufzuordnung aller Leitungen anzeigen**

Parameter	Beschreibung
Leitung	Anzeige der an das Kommunikationssystem angeschlossenen physikalischen Amtsleitung.
Box-Sl-Pt-Le oder Box/Slot/Port/Leitung	Anzeige des Baugruppentyps sowie die Einbauplatz- und Port-Nummer (physikalischen Port) für den Anschluss der Leitung an das Kommunikationssystem.
Tag Ruf-Nr.	Anzeige der zugewiesene Rufnummer für Tagbetrieb
Tag Name	Anzeige des Namens der zugewiesenen Rufnummer für Tagbetrieb
Nacht Ruf-Nr.	Anzeige der zugewiesene Rufnummer für Nachtbetrieb
Nacht Name	Anzeige des Namens der zugewiesenen Rufnummer für Nachtbetrieb

Parameterbeschreibung der Registerkarten:

- **Leitung hinzufügen**

Parameter	Beschreibung
Anzahl	Anzahl der hinzuzufügenden Leitungen.

Parameterbeschreibung der Registerkarten:

- **Leitung ändern**
- **Leitung löschen**

Parameter	Beschreibung
Leitung	Anzeige der Leitungsnummer.
Box/Slot/Port/Leitung	Anzeige des physikalischen Ports der Leitung (Box/Slot/Port/Leitung).
Kennzahl	Anzeige oder Eingabe der Richtungskennzahl.
Richtung	Anzeige oder Auswahl der Richtung, die der Leitung zugeordnet ist (keine oder Rtg.1 bisi Rtg.12).
Rufzuordnung Leitung	
Tag Ruf-Nr.	Rufnummer für nicht durchwahlfähige kommende Verbindung am Tag.
Nacht Ruf-Nr.	Rufnummer für nicht durchwahlfähige kommende Verbindung am Nachtbetrieb.

Parameterbeschreibung der Registerkarten:

- **ISDN-Flags ändern**

Parameter	Beschreibung
Protokoll: Beschreibung	Jeder Eintrag für ein Protokoll-Template setzt sich zusammen aus Interface, Protokoll und Zusatzinfo: S0 Basisanschluss 2B+D über S0 -Interface, BRI Basisanschluss 2B+D über U2B1Q -Interface (USA), S2 Primärmultiplexanschluss 30B+D, T1 Primärmultiplex-anschluss 23B+D (USA)
Logical/Physical	logische oder physikalische Zählweise der Kanäle
Slave B-channel neg: Master	Festlegung Master/Slave innerhalb des Layer 3. Bei Verbindungen ist eine Seite als Slave - die andere Seite als Master einzustellen.
Up B-channel alloc: Down	Festlegung der B-Kanalzählweise (muss in beiden Systemen gleich sein)
S0 CHI format: S2M	Protokollformat CHI, festzulegen als S0 (kurzes Format) oder S2M (langes Format)
Unsymmetric/Symmetric	Symmetrische bzw. nicht symmetrische Verwendung von L3-Protokollelementen
Automatic/Fixed	Automatische Aushandlung bzw. Feste Zuordnung der Symmetrie
1 CR length: 2	Protokollformat Call Referenzlänge
Alarm signalling	Verwendung von Alarm-signalisierungen im Schicht 3 Protokoll
Protocol timers	Verwendung der Schicht 3 Timer
PRI quickstart	Verwendung der PRI-Quickstart Prozedur
IE_TNS	Verwendung des Informationselements Transit Network Selection
IE_OSA	Verwendung des Informationselementes Open Service Access
CIDL	Verwendung der Call and Link ID-Signalisierung in der Vernetzung
Userside/Networkside	Protokollfestlegung Layer 2. Auf der Gegenseite gespiegelte Einstellung notwendig
Network/Subscriber	Protokollfestlegung Layer 2. Auf der Gegenseite gespiegelte Einstellung notwendig
PP/PMP	Festlegung Punkt zu Punkt oder Punkt zu Mehrpunkt, nur bei S0 relevant
Permanent active	Schicht 2 Daueraktiv
Active TEI verify	TEI Überprüfung aktivieren
Userside/Networkside	Protokollfestlegung Layer 1. Auf der Gegenseite gespiegelte Einstellung notwendig
PP/PMP	Protokollfestlegung Layer 1. Gleiche Einstellungen auf beiden Seiten notwendig

Parameter	Beschreibung
S Bus type: L	kurzer/langer Bus (Reichweiten)
Permanent active	Protokollfestlegung Layer 1. Gleiche Einstellungen auf beiden Seiten notwendig
CRC4 check	Protokollfestlegung Layer 1., nur bei S2M relevant, beide Seiten gleiche Einstellung
CRC4 reporting	Protokollfestlegung Layer 1., nur bei S2M relevant, beide Seiten gleiche Einstellung

Parameterbeschreibung der Registerkarten:

- **B-Kanal ändern**

Parameter	Beschreibung
B-Kanal	Anzeige der B-Kanalnummer.
gehend	Auf dem B-Kanal darf gehend telefoniert werden.
kommend	Auf dem B-Kanal darf kommend telefoniert werden.

27.3.10.2 Leitungen/Vernetzung > Richtung

Parameterbeschreibung der Registerkarten:

- **Richtung ändern**

Parameter	Beschreibung
Richtungsname	Name der Richtung. Der eingegebene Name tritt nun an die Stelle der standardmäßig eingerichteten Richtungsnummer in der Liste Richtungen.
Richtungskennzahlen	Hier werden die Belegungskennzahlen für jede Richtung eingegeben. Die eingegebenen Richtungskennzahlen müssen untereinander und innerhalb des gesamten Rufnummernplans des Kommunikationssystems kollisionsfrei sein. Zum Test auf Kollisionsfreiheit dient die Schaltfläche "Prüfen". Durch Wahl der Belegungskennzahl wird die Vermittlungsanlage veranlasst, dem betreffenden Teilnehmer eine Leitung zuzuweisen. Richtungskennzahlen greifen nur, wenn LCR nicht aktiv ist.
Amtskennziffer (2. AKZ)	Eine zweite Amtskennziffer wird dann definiert, wenn das Kommunikationssystem eine Unteranlage eines anderen Kommunikationssystems ist oder mit mehreren anderen Kommunikationssystemen vernetzt ist. Sie ist nur für Vernetzungs-Richtungen (Richtungsart=PABX) relevant. In diesem Fall dient die zweite Amtskennziffer als Belegungskennzahl für die Hauptanlage. Innerhalb einer Vernetzung sind die Kennzahlen für die Amtsbelegung, die Richtungskennzahl(en) und die zweite Amtskennziffer einheitlich zu konfigurieren. Standard in Deutschland ist 0.
Gateway-Standort	
Ländervorwahl	Anzeige der Ländervorwahl des eigenen Gateway-Standorts. Einstellung über Grundeinstellungen/Gateway/Gateway Standorte
Ortsnetzkennzahl	Anzeige der Ortsnetzkennzahl des eigenen Gateway-Standorts. Einstellung über Grundeinstellungen/Gateway/Gateway Standorte
Anlagenrufnummer	Anzeige der Anlagenrufnummer des eigenen Gateway-Standorts. Einstellung über Grundeinstellungen/Gateway/Gateway Standorte
Anlagenrufnummer-kommend	

Parameter	Beschreibung
Ländervorwahl	Dient zur Wahlbewertung bei kommenden Rufen. Ländervorwahl ohne führende Nullen (z. B. 1 in USA, 49 in Deutschland)
Ortsnetzkennzahl	Dient zur Wahlbewertung bei kommenden Rufen. Ortsnetzkennzahl ohne führende Nullen (z. B. 89 für München)
Anlagenrufnummer	Dient zur Wahlbewertung bei kommenden Rufen. Anlagenrufnummer (zentrale Firmenrufnummer, z. B. 777)
Standort-Nummer	Dient zur Wahlbewertung öffentlicher Rufnummern bei gehenden Verbindungen. Abprüfung der Wahlinformation, ob sich die gerufene Zielrufnummer in der eigenen Anlage befindet.
Anlagenrufnummer-gehend Info: Änderungen bei den Anlagerufnummern-gehend müssen mit den Netzprovidern abgestimmt sein. (Clip no screening)	
Ländervorwahl	Dient zur Anruferidentifizierung bei gehenden Rufen. Ländervorwahl ohne führende Nullen (z. B. 1 in USA, 49 in Deutschland) wird an das Netz übertragen. Ist keine Anlagenrufnummer-gehend eingetragen, wird automatisch die Anlagenrufnummer-kommend verwendet.
Ortsnetzkennzahl	Dient zur Anruferidentifizierung bei gehenden Rufen. Die hier angegebene Ortsnetzkennzahl (ohne führende Nullen, z. B. 89 für München) wird an das Netz übertragen. Ist keine Anlagenrufnummer-gehend eingetragen, wird automatisch die Anlagenrufnummer-kommend verwendet.
Anlagenrufnummer	Dient zur Anruferidentifizierung bei gehenden Rufen. Die hier angegebene Anlagenrufnummer (zentrale Firmenrufnummer, z. B. 777) wird an das Netz übertragen. Ist keine Anlagenrufnummer-gehend eingetragen, wird automatisch die Anlagenrufnummer-kommend verwendet.
TIn-RufNr unterdrücken	Die Anruferidentifizierung erfolgt bei aktiviertem Flag ohne Durchwahlnummer.
Überlaufrichtung	
Überlaufrichtung	Falls alle Leitungen der konfigurierten Richtung belegt sind, kann ein Überlauf auf andere Richtungen eingestellt werden. Die Überlaufrichtung gilt nur bei deaktiviertem LCR
Wahlaussendung	
Wahlaussendung	Die Art der Wahlaussendung wird hier für die ausgewählte Richtung festgelegt und unter Einstellungen | Automatische Wegesuche | Wahlplan nach der Auswahl der Wegetabelle (siehe Klappliste Wegetabelle) als statischer Text (z. B. Wegetabelle 6: Blockweise) angezeigt.
Wahlaussendung: Schritthaltend	Die Aussendung der Ziffern erfolgt synchron zur Wahl.

Parameter	Beschreibung
Wahlaussendung: Blockweise	Bei blockweiser Wahlaussendung (Blockwahl pro Richtung) werden die gewählten Ziffern vom Kommunikationssystem zwischengespeichert. Die Wahl erfolgt erst nach Ablauf eines Timers nach der letzten gewählten Ziffer oder nach Eingabe des Wahlendekennzeichens #. Bei PRI in USA ist Blockwahl zum Amt vorgeschrieben. Um blockweise Wahlaussendung auswählen zu können, muss die automatische Wegesuche (LCR) aktiviert sein. In der LCR-Wegetabelle wird die Art der Wahlaussendung automatisch auf blockweise Wahlaussendung gesetzt, wenn mindestens eine Richtung der LCR-Wegetabelle mit blockweiser Wahlaussendung konfiguriert ist.
Mobile Nebenstellenummer (MEX)	
MEX-Nummer	Falls der genutzte ITSP das Leistungsmerkmal "Mobile Extension (MEX)" unterstützt, muss hier die MEX-Nummer (8-stellig, nur Ziffern) eingegeben werden, die vom ITSP zur Verfügung gestellt wird. Dieses Leistungsmerkmal ist nur mit einem Internet-Telefonie-Durchwahlanschluss (SIP like ISDN) nutzbar. Damit werden Mobiltelefone/Smartphones in das Kommunikationssystem integriert. Der Benutzer des Mobiltelefons ist über den One Number Service unter einer einzigen Rufnummer erreichbar, die auch dem Gesprächspartner übermittelt wird. Telefoniert der Teilnehmer mit seinem Mobiltelefon, wird dem Gesprächspartner z. B. die Büronummer des Teilnehmers angezeigt, die Nummer des Mobiltelefons bleibt unbekannt. Zusätzlich können andere Teilnehmer den Anwesenheitsstatus des Teilnehmers abfragen, auch wenn er gerade mit seinem Mobiltelefon telefoniert.

Parameterbeschreibung der Registerkarten:

- **Richtungsparameter ändern**

Parameter	Beschreibung
Richtungsflags	
Ziffernwiederholung ein	Bei gehender Richtungsbelegung mit eingeschalteter Ziffernwiederholung wird die Richtungskennzahl vor der Rufnummer ausgesendet. Dies gilt nur bei ausgeschaltetem LCR (siehe Einstellungen | Automatische Wegesuche).
Auswertung 2. Hörzeichen / Leitungsüberwachung	Mit dieser Option wird das Kommunikationssystem in die Bereitschaft versetzt einen zusätzlichen Wählton zu erkennen. Diese Funktion wird beim Einsatz von Kommunikationssystemen im Tandembetrieb benutzt. Die Auswertung erfolgt länderabhängig, z.B. in Belgien nach 00 und in Frankreich nach 16 bzw. 19. In Deutschland ist dies nicht relevant. Dies gilt nur bei öffentlichen Netzbetreibern, die bei Auslandsgesprächen einen zweiten Wählton senden.
Abwurf pro Richtung	Dieses Flag wird benötigt für QSIG-Vernetzungen. Ist das Flag gesetzt, prüft das Kommunikationssystem, ob die Gegenseite zum Abwurf aufgefordert wird oder ob das Kommunikationssystem ein Forward switching zum zentr. Abwurfplatz durchführt. Es wird der Gegenseite eine Meldung gesendet, in der gesagt wird, ob die Gegenseite einen Abwurf für diesen Ruf durchführen soll oder nicht. Wird in einer Richtung ein Abwurf ausgelöst, so erfolgt er zum Abwurfplatz in dieser Richtung. Die Realisierung dieses Leistungsmerkmals bedingt, dass für jede Richtung Tag- und Nacht-Rufnummern eingerichtet sind (siehe Rufzuordnung Ltg) und dass kein Abwurfplatz für die Tag- und Nachtschaltung eingetragen ist (siehe Abwurf/VPL).

Parameter	Beschreibung
Üb.-Dienst 3,1 kHz Audio	Bei allen gehenden Verbindungen über ISDN ist Üb.-Dienst 3,1 kHz Audio die Standardeinstellung. Dies ist die Standard-Übertragungsart für gehende Verbindungen über eine ISDN-Leitung (die Abkürzung Üb.- steht hierbei für Übertragung). Verbindungen zwischen dem Kommunikationssystem und digital vermittelnden Ämtern über ein analoges Modem werden als Datendienst gekennzeichnet. Um Probleme beim FAX-Betrieb zu vermeiden, sollte dieses Flag gesetzt sein. In einigen Fällen unterstützt ein Netzbetreiber die Übertragungsart Dienst 3,1 kHz Audio nicht. Dies kann dazu führen, dass die Faxübermittlung zu gewissen externen Rufnummern fehlschlägt. Eine Lösungsmöglichkeit ist, das Flag **Üb.-Dienst 3,1 kHz Audio** zu deaktivieren.
Rtg.-Präfix ergänzen kommend	Mit aktivierter Option wird bei Systemtelefonen bei kommender Belegung die Rufnummerndarstellung um die Richtungskennzahl ergänzt.
Rtg.-Präfix ergänzen gehend	Mit aktivierter Option wird bei gehender Belegung die Rufnummerndarstellung um den AccessCode ergänzt. Info: Änderungen des Parameters bewirken eine Modifizierung der Anruferidentifizierung und müssen mit den Netzprovidern abgestimmt sein. (Clip no screening)
Rufnr. mit internationalem / nationalem Präfix	Ist dieses Flag aktiviert, muss für den ITSP die nationale bzw. die internationaler Kennziffer der Rufnummer vorangestellt werden (z. B. 02302…., 00492302...). Standard: Aktiviert
Freiton zum Amt	Bei kommendem Amtsanruf auf ISDN-Leitungen wird bei gesetztem Flag im entsprechenden Verbindungszustand ein Freiton zum Amt gesendet. Dieses Flag ist als Protokoll-Sonderbehandlung beim Netzbetreiber Global One und Sovintel-Ämtern zu setzen.
Segmentierung	Hier wird das Verhalten des Systems festgelegt, wenn ISDN-Nachrichten versendet werden, die die maximale Schicht 2 Nutzdatenlänge (260 Byte) überschreiten.
Segmentierung: ja	Die zu versendende Nachricht wird in 260 Byte große Segmente aufgeteilt und einzeln versendet. Das empfangende Kommunikationssystem muss die Segmentierung unterstützen und diese einzelnen Segmente aufsammeln und zu einer Nachricht zusammensetzen.
Segmentierung: nein	Eine Segmentierung ist nicht notwendig, da die unterliegende Schicht 2 beliebig lange Nachrichten transportieren kann.
Segmentierung: Truncate Message	Die zu versendende Nachricht wird um weniger wichtige Anteile (z.B. Namen) auf kleiner 260 Byte gekürzt und versendet.
UUS pro Richtung deaktivieren	Die „Teilnehmer zu Teilnehmer-Signalisierung“ (User to User Signaling, UUS) kann über dieses Flag deaktiviert werden. Damit wird bei einer externen Anrufumleitung (AUL ext.) die Übermittlung von Name und Rufnummer des A-Teilnehmers im UUI-Element (User-to-User Information, UUI) unterdrückt. Dieses Flag muss für Telefonica deaktiviert werden.
immer DSP benutzen	Ist dieses Flag gesetzt, ist eine Verbindung zum Internet-Telefonie Service Provider nur über einen DSP (Digitaler Signalprozessor) möglich. Ist dieses Flag nicht gesetzt, gibt es eine „Direct Payload“-Verbindung zum Internet-Telefonie Service Provider. Für die Richtung der OpenScape Voice-Vernetzung muss dieses Flag gesetzt sein. Bei Fax-Übertragungen (T.38) über ein externes Gerät (z. B. Mediatrix 4102) darf dieses Flag nicht gesetzt sein.

Parameter	Beschreibung
Pause vor Wahl	Hier können verschiedene Zeiten ausgewählt werden, die den Wahlbeginn bei analogen Wählleitungen (HKZ) bestimmen. Wird Hörtonauswertung (keine Pause) aktiviert, wartet das Kommunikationssystem, bis ein Wählton erkannt wird. Anmerkung für Brasilien Wird das MFV-Wahlverfahren von analogen Endgeräten aus verwendet, und zwar in Verbindung mit analogen Amtsleitungen und Impulswahlverfahren nach der Hörzeichenüberwachung, kann es Probleme mit der Wahlkontrolle geben, wenn die Ländervorwahl auf Brasilien eingestellt ist. In diesem Fall gehen die MFV-Signale von den analogen Endgeräten direkt zu den analogen Amtsleitungen (das „1A-Verfahren“ wird nicht verwendet). Aus diesem Grund gehen alle MFV-Signale verloren, die vor dem Empfang des Wähltons gewählt werden. Hier muss die automatische Wegesuche (LCR) für eine einwandfreie Funktion von Wahlverfahren und Wahlkontrolle des Endgeräts aktiviert sein.
Amtsrufpause	Die Amtsrufpause gibt an, nach welcher Zeit das Rufende erkannt wird, wenn der Amtsruf nicht fortgesetzt wird. Dieser Eintrag gilt nur für HKZ-Leitungen. Bei einem Amtsruf von beispielsweise 1 s Ruf, 4 s Rufpause ist eine Anrufpause von 6 s zu konfigurieren. Bei einigen Ämtern gibt es jedoch eine Rufpause von ca. 10 s. Hierbei muss dann eine Anrufpause von 13 s programmiert werden, andernfalls erfolgt keine Rufweiterschaltung. In den USA umfasst dieser Rhythmus zwei Sekunden Ruf und zwei Sekunden Rufpause, insgesamt also eine Dauer von sechs Sekunden. Der Sechs-Sekunden-Zyklus dient als Standardeinstellung, sodass hier keine Änderungen vorgenommen werden müssen. Einstellbereich: 2 bis 13 Sekunden.
Belegungsart	Für eine gehende Richtungsbelegung wird hier festgelegt, nach welchen Kriterien das Kommunikationssystem eine freie Leitung in der entsprechenden Richtung sucht.
Belegungsart: zyklisch	Das Kommunikationssystem beginnt die zyklische Suche nach einer freien Leitung bei der nächsthöheren Leitungsnummer, bezogen auf die zuletzt gehend belegte Leitung in dieser Richtung.
Belegungsart: Linear	Das Kommunikationssystem beginnt die Suche stets bei der niedrigsten Leitungsnummer, die dieser Richtung zugeordnet ist.
Richtungsart	Bei Richtungsart stehen zwei Optionen zur Verfügung. Als Richtungsart kann entweder Amt oder PABX (Private Automatic Branch Exchange = private Nebenstellenanlage) eingestellt werden.
Richtungsart: Amt	Auf Leitungen, die dieser Richtung zugeordnet sind, wird eine Wahlkontrolle durchgeführt. Wenn LCR aktiv ist, wird die Wahlkontrolle über Wahlplan (Spalte Wako) geregelt.
Richtungsart: PABX	Eine Wahlkontrolle wird nur dann durchgeführt, wenn dieser Richtung eine zweite Amtskennzahl zugeordnet ist. Wenn LCR aktiv ist, wird die Wahlkontrolle über Wahlplan (Spalte Wako) geregelt. Die Richtungsart hat auch einen Einfluss auf den Standardtext des Richtungsnamens (siehe Richtungen), sowie auf das Verfahren, welches bei der Erkennung des Hörzeichens auf HKZ-Leitungen angewendet wird.
Nr-Typ, gehend	Der Administrator kann die Anlagenrufnummer kommend und gehend getrennt festlegen, aufgeteilt in die Anteile Ländervorwahl, Ortsnetzkennzahl und Anlagenrufnummer (=Anschlussnummer im Ortsnetz) . Dies wird für die Realisierung des Leistungsmerkmals CLIP no screening benötigt. Ist keine Anlagenrufnummer gehend konfiguriert, verwendet das Kommunikationssystem stets die Daten der Anlagenrufnummer kommend. Bei einer kommenden Belegung auf einer ISDN-Leitung blendet das Kommunikationssystem aus der empfangenen Rufnummer die Anlagenrufnummer linksbündig aus und interpretiert den verbleibenden Teil als Durchwahlnummer. Bei Rufnummerninformationen an das PSTN setzt das Kommunikationssystem die Anlagenrufnummer (bzw. den per Konfiguration definierten Anteil davon) automatisch als führenden Teil der Rufnummer ein. Dieses gilt nicht für die Wahlinformation (Destination Address). Die Rufnummer interner Teilnehmer, die zur Gegenstelle gesendet wird, kann sich folgendermaßen zusammensetzen:

Parameter	Beschreibung
Nr-Typ, gehend: Unbekannt	nur Durchwahlnummer (Standardeinstellung)
Nr-Typ, gehend: Anlagenrufnummer	Anlagenrufnummer + Durchwahlnummer
Nr-Typ, gehend: Ortsnetzkennzahl	Ortsnetzkennzahl + Anlagenrufnummer + Durchwahlnummer
Nr-Typ, gehend: Ländervorwahl	Ländervorwahl + Ortsnetzkennzahl + Anlagenrufnummer + Durchwahlnummer
Nr-Typ, gehend: Intern	nur für vernetze Systeme: bei einem geschlossenen Rufnummernplan soll u.U. kein Nummern-Präfix ergänzt werden. Hier wird eine Rufnummernergänzung unterdrückt.
Rufnummer Typ	Die Einstellungen im Bereich Nr-Typ, gehend beeinflussen auch Anrufe, die von einer Nebenstelle in einer Partneranlage (einem vernetzten Knoten) kommen.. Die Rufnummer des Anrufers, die vom vernetzten Knoten empfangen und an das Amt weitergeleitet wird, wird aufgrund dieser Einstellung für die gehende Richtung erweitert.
Rufnummer Typ: Intern	Hier wird nur eine Information über die interne Rufnummer gesendet. Ist der Zielteilnehmer Extern, wird entweder keine oder die Vermittlungsplatz-Rufnummer gesendet. Bei internen Zielteilnehmern in einem anderen Knoten kann die interne Rufnummer angezeigt werden.
Rufnummer Typ: Durchwahl	Hier wird nur eine Information über die DuWa-Nummer versendet. Bei internen Zielteilnehmern in einem anderen Knoten fehlt für eine Displayanzeige die interne Rufnummer. Für externe Ziele ist die Rufnummerninformation ausreichend.
Rufnummer Typ: Intern / DuWa	In einer Vernetzung ist es sinnvoll diese Einstellung zu wählen. Dem Zielteilnehmer werden sowohl die interne als auch die DuWa-Rufnummer gesendet. Wird in der Vernetzung ein interner Teilnehmer gerufen, kann diesem Teilnehmer die interne Rufnummer des Rufers angezeigt werden. Hat der interne Zielteilnehmer beispielsweise eine Anrufumleitung an ein externes Ziel aktiviert, so kann in diesem Fall eine DuWa-Rufnummer mitgesendet werden.
Rerouting	
Richtungswechsel erlaubt	Bei aktiviertem Flag lassen sich D-Kanal-Informationen auch über andere Richtungen routen. Diese Option erlaubt ein alternatives Routing über andere Richtungen. Die Option darf nur bei eindeutigem Rufnummernplan aktiviert werden. (Verdeckte Nummerierung oder eindeutige Richtungskennzahlen im Netzverbund. Das auffordernde Kommunikationssystem muss dies auch unterstützen). Wird ein Rerouting über eine andere Richtung gemacht, muss auch für die entsprechende Richtung Rerouting mit Richtungswechsel aktiv sein. Diese Option ist nur bei CorNet NQ-Vernetzung verfügbar und muss bei beiden vernetzten Kommunikationssystemen identisch eingestellt sein.
Rerouting aktiv	Zur Optimierung der B-Kanal-Ausnutzung kann eine Anrufumleitung über das Protokoll entsprechend der Spezifikation Call Forwarding/Partial Rerouting durchgeführt werden. Bei Rückweisung von Partial Rerouting wird auf Forward Switching zurückgegriffen.

Parameter	Beschreibung
Rerouting aktiv: Nein	Bei dieser Option ist Rerouting ausgeschaltet. Bei einer Anrufumleitung wird die Verbindung immer über zwei B-Kanäle aufgebaut.
Rerouting aktiv: Falls Weg bekannt	Bei dieser Option ist Rerouting nur dann aktiv, wenn der Weg bekannt ist und wenn zwischen den beiden vernetzten Kommunikationssystemen ein erfolgreiches Handshaking stattfindet.
Rerouting aktiv: Immer	Bei dieser Option weist das Kommunikationssystem eine Verbindung zurück, wenn die Setup-Meldung für die kommende Verbindung über die selbe Richtung eingeht wie die Anrufumleitungsziel-Richtung. Die Option Immer ist nur bei CorNet NQ-Vernetzung verfügbar und muss bei beiden vernetzten Kommunikationssystemen identisch eingestellt sein.

Parameterbeschreibung der Registerkarten:

- **Spezial Parameter ändern**

Parameter	Beschreibung
Nummerierungsplan Bestimmt den Parameter Numbering Plan in ausgehenden Meldungen	
Called Party Number	System-Kontrolle= wird vom System festgelegt, ISDN-Nummerierungsplan, Privater Nummerierungsplan, Unbekannter Nummerierungsplan= manuell vorgegebene Einstellung
Alle Anderen	z.B. Calling Party No., Redirecting No, etc. System-Kontrolle= wird vom System festgelegt. ISDN-Nummerierungsplan, Privater Nummerierungsplan, Unbekannter Nummerierungsplan= manuell vorgegebene Einstellung
Standort-Angabe	Der Parameter Standortangabe (Location)legt fest, wie im Q931-Infoelement CAUSE und Progress Indicator der Parameter Location gesetzt wird. System-Kontrolle= wird vom System festgelegt, alternativ kann die Einstellung „Privates Netz und Teilnehmer“ oder „Immer Teilnehmer“ manuell erfolgen.
COLP	Ist dieses Flag gesetzt, bekommt der Anrufer bei einer extern kommenden Amts-Verbindung die Rufnummer des Angerufenen angezeigt. Somit kann der Anrufer feststellen, ob die Verbindung weitergeleitet wurde oder von einem anderen Teilnehmer übernommen wurde. Dieses Leistungsmerkmal muss im Amt ebenfalls freigegeben sein. Das Leistungsmerkmal ist nur bei digitalen Leitungen verfügbar (BRI bzw. PRI). Wird bei gesetztem Flag ein extern kommender Ruf weitergeleitet oder abgefragt, so wird in der vom Kommunikationssystem abgehenden Connect-Meldung die aktualisierte Rufnummer zum Amt signalisiert. Falls das Leistungsmerkmal COLP im Amt freigeschaltet ist, wird die aktualisierte Rufnummer auch beim Anrufer dargestellt. Info: Das Flag wirkt nicht auf die Rufnummerndarstellung bei extern gehenden Verbindungen.
Notify senden	Diese Meldung dient zur Übermittlung von Statusinformationen zur aktuellen Verbindung. Die Meldung kann sowohl vom Netz als auch vom Teilnehmer gesendet werden, um die andere Seite (Netz oder Teilnehmer) z.B. über eine Verbindungsunterbrechung oder über eine aktivierte Anrufumleitung zu informieren. Wenn ein Amt das Notify nicht unterstützt, kann durch Zurücksetzen des Flags die Notify-Meldung unterdrückt werden. Bei aktiver Option wird eine “Notify”-Meldung zur Mitteilung von z.B. Halten oder Parken gesendet. Notify senden wird nur in den Protokollen DSS1, NI1 und MCI ausgewertet. In den Protokollen SIP-Q, CorNet-NQ und QSIG wird die Notify-Information dagegen immer gesendet.

Parameter	Beschreibung
Ohne CLIP	Ist dieses Flag gesetzt, wird bei gehenden Verbindungen auf der BRI- bzw. PRI-Leitung die Anruferidentifikation ins öffentliche Netz unterdrückt. Dieses Flag lässt sich einzeln für unterschiedliche Richtungen aktivieren bzw. deaktivieren. Zusätzlich hat der Teilnehmer die Möglichkeit, die Anruferidentifikation für einzelne Gespräche über eine Berechtigungskennzahl oder über das Menü des Systemtelefons zu unterdrücken.
Kein SETUP ACK.	Ist dieses Flag gesetzt, wird die Setup-Acknowledgement-Meldung vom Kommunikationssystem ins Amt unterdrückt. Relevant für spezielle Ämter. Beispiel: Fetex150-Ämter von Fujitsu.
Kein DIV.LEG-Info	Wenn dieses Flag gesetzt ist, wird die sonst übliche Diverting-LEG-Information (Rufnummer des umleitenden Teilnehmers) nicht zum Amt gesendet. Die DIV.-LEG-Infosollte dann unterdrückt werden, wenn Probleme bei der externen Anrufumleitung (AUL ext.) auftreten.
Mit sending complete	Ist dieses Flag gesetzt, wird die optionale Information "Alle Ziffern gesendet" vom System ausgegeben, nachdem alle gewählten Ziffern ausgesendet wurden.

27.3.10.3 Leitungen/Vernetzung > QSIG-Leistungsmerkmale

In einem aus mehreren Kommunikationssystemen bestehenden Netzverbund werden in den Teilanlagen anfallende Verbindungsinformationen (GEZ-Daten) an ein festgelegtes Kommunikationssystem des Verbunds gesendet. Zu diesem Zweck wird in jedem Kommunikationssystem die Rufnummer des Zielsystems (Rufnummer der zentralen Erfassungsstelle) konfiguriert, an das die Verbindungsdaten gesendet werden.

Parameterbeschreibung der Registerkarten:

- **QSIG-Leistungsmerkmale ändern**

Parameter	Beschreibung
Daten der eigenen Anlage	
Anlagennummer	Mit diesen Daten wird das eigene Kommunikationssystem im Netzverbund identifiziert. Diese Daten sind sowohl für die zentrale Besetztsignalisierung als auch für das Verbindungsdaten-Routing gültig. In einem aus mehreren Kommunikationssystemen bestehenden Netzverbund hat jedes Kommunikationssystem eine eindeutige Anlagennummer. Wenn das Kommunikationssystem mit solchen Kommunikationssystemen vernetzt ist, und man möchte die QSIG-Leistungsmerkmale benutzen, dann muss aus Kompatibilitätsgründen auch hier die Anlagennummer administriert werden. Wertebereich: 1 bis 255
Gruppennummer	In den Kommunikationssystemen können die Teilnehmer in Gruppen eingeteilt werden, die dann eine eindeutige Gruppennummer erhalten. Im Kommunikationssystem existiert eine solche Gruppierung nicht. Trotzdem soll aus Kompatibilitätsgründen auch hier die Gruppennummer administriert werden. Wertebereich: 1 bis 40
Anlagenübergreifende Besetztsignalisierung	

Parameter	Beschreibung
Anlagen-Nr. Zielsystem	Mit diesen Daten wird ein Kommunikationssystem definiert, das die zentrale Besetztsignalisierung realisiert. Dies kann sowohl die Hauptanlage als auch eine Unteranlage sein. Anlagennummer des Kommunikationssystems, das für die zentrale Besetztsignisierung eingerichtet ist. Wertebereich: 1 bis 255
Ruf-Nr. Zielsystem	Rufnummer des Kommunikationssystems, das für die zentrale Besetztsignisierung eingerichtet ist. Hier ist nur die Anlagenrufnummer und keine Teilnehmerrufnummer einzutragen. Im LCR-Wahlplan ist zu berücksichtigen, dass beim Eintrag für diese Anlagenrufnummer keine Nachwahl eingetragen wird! Beispiel: Die Rufnummer des Zielsystems sei: 999 Der Wahlplaneintrag muss dann sein: -999 (und nicht -999XXX und nicht -999Z).
Verbindungsdaten-Routing	
Ruf-Nr. Zielsystem	Mit diesen Daten wird ein Kommunikationssystem definiert, das die zentrale Verbindungsdatenerfassung realisiert. Dies kann sowohl die Hauptanlage als auch eine Unteranlage sein. Rufnummer des Kommunikationssystems, das als zentrale Erfassungsstelle eingerichtet ist (siehe auch den Hinweis zu Ruf-Nr. Zielsystem, weiter oben).

27.3.10.4 Leitungen/Vernetzung > MSN zuweisen

Parameterbeschreibung der Registerkarten:

- **MSN anzeigen**
- **MSN ändern**

Parameter	Beschreibung
MSN	Anzeige oder Eingabe der MSN (Mehrgeräteanschluss Rufnummer).
Leitung	Anzeige der Zuordnung der Leitung, auf der die MSN aktiv ist.

27.3.10.5 Leitungen/Vernetzung > ISDN-Parameter

Durch den Referenztakt (ISDN Clock) werden Abläufe auf Amtsleitungen innerhalb eines bestimmten Netzes oder innerhalb des Amts synchronisiert. Normalerweise sucht sich das Kommunikationssystem automatisch die Leitung aus, die als Referenztaktgeber für sämtliche Kommunikationssysteme innerhalb eines Netzes oder im Amt fungiert. Sollte die Referenztaktleitung jedoch einmal ausfallen, müssen eine oder mehrere andere Leitungen als Referenztaktgeber eingerichtet werden.

Das Kommunikationssystem wählt die Leitung nach folgender Rangfolge aus:

1. Erlaubnisliste
2. S_{2M}-Amtsleitung

3. S_0-Amtsleitung
4. S_{2M}-Querleitung (nur Slave-Konfiguration)
5. S_0-Querleitung

Parameterbeschreibung der Registerkarten:

- ***!ISDN Clock**

Parameter	Beschreibung
Index	Die Positionen spiegeln die Prioritäten 1-4 (für Erlaubnisliste) bzw. 1-16 (für Verbotsliste) wider.
Erlaubnislisten	Beinhaltet die Erlaubnisliste Einträge, wird die automatische Leitungsauswahl des Kommunikationssystems außer Kraft gesetzt. Die in der Erlaubnisliste eingetragenen ISDN-Ports (max 4 möglich) werden bei der Suche nach der Referenztaktleitung als Erstes verwendet.
Verbotslisten	Die in der Verbotsliste eingetragenen ISDN-Ports (max 16 möglich) werden bei der Suche nach der Referenztaktleitung übergangen.

27.3.11 Berechtigungen

Unter **Berechtigungen** sind die Funktionen für die Berechtigungen der Amtsleitungen zusammengefasst. Sie regeln den Zugang der Teilnehmer zu möglicherweise kostenpflichtigen externen Verbindungen.

27.3.11.1 Berechtigungen > Teilnehmer

Parameterbeschreibung der Registerkarte:

- **Alle Teilnehmer anzeigen**

Parameter	Beschreibung
Ruf-Nr., **Rufnummer**	Rufnummer des Teilnehmers.
Name	Namen des Teilnehmers.
Tag	Ausgewählte Berechtigungsgruppe für den Tag.
Nacht	Ausgewählte Berechtigungsgruppe für die Nacht.
Berechtigungsgruppe Tag	Auswahl der Berechtigungsgruppe für den Tag. Die vorgenommene Auswahl verweist auf die Tabelle **Berechtigungen Tag**, über die die Berechtigungsgruppe mit der tatsächlichen Berechtigung verknüpft wird.
Berechtigungsgruppe Nacht	Auswahl der Berechtigungsgruppe für die Nacht. Die vorgenommene Auswahl verweist auf die Tabelle **Berechtigungen Nacht**, über die die Berechtigungsgruppe mit der tatsächlichen Berechtigung verknüpft wird.

27.3.11.2 Berechtigungen > Tag: Berechtigungsgruppen

Parameterbeschreibung der Registerkarten:

- **Namen ändern**
- **Berechtigungsgruppe ändern**
- **Tag: Gruppenmitglieder anzeigen**

Parameter	Beschreibung
Berechtigungsgruppe	Selbstgewählter Name für die Berechtungsgruppen 1 bis 15. Zuweisung von Amtsberechtigungen pro Richtung (Leitungsbündel) jeweils für Tag und Nacht. Bei der Konfiguration der Teilnehmer kann der Zugriff auf externe Rufnummern durch Zuweisung von Berechtigungsgruppen eingeschränkt werden.
Berechtigung	Zuweisen der Berechtigungen zu den einzelnen Berechtigungsgruppen für Tagbetrieb. Alle Einschränkungen werden nur wirksam an Leitungen einer Richtung des Typs Amt.
Berechtigungsgruppe: Intern	Der Teilnehmer darf nur intern telefonieren. Standardwert: Default in Berechtigungsgruppe 1
Berechtigungsgruppe: Halbamt	Der Teilnehmer darf externe Gespräche nur annehmen. Standardwert: Default in Berechtigungsgruppe 2
Berechtigungsgruppe: Erlaubnisliste	Der Teilnehmer darf nur die in der Erlaubnisliste definierten externen Rufnummern wählen. Ist keine Rufnummer eingetragen gilt Halbamtsberechtigung. Standardwert: Default in Berechtigungsgruppe 4
Berechtigungsgruppe: Verbotsliste	Der Teilnehmer darf die in der Verbotsliste definierten externen Rufnummern nicht wählen. Ist keine Rufnummer eingetragen gilt Vollamtsberechtigung. Standardwert: Default in Berechtigungsgruppe 3, 5, 6
Berechtigungsgruppe: Vollamt	Der Teilnehmer darf ohne Einschränkung kommende und gehende externe Gespräche annehmen und aufbauen. Standardwert: Default in Berechtigungsgruppe 7 bis 15
Gruppenmitglieder anzeigen	Anzeige von Rufnummer und Name der Mitglieder in der ausgewählten Berechtigungsgruppe.

27.3.11.3 Berechtigungen > Nacht: Berechtigungsgruppen

Parameterbeschreibung der Registerkarten:

- **Namen ändern**
- **Berechtigungsgruppe ändern**
- **Nacht: Gruppenmitglieder anzeigen**

Parameter	Beschreibung
Berechtigungsgruppe	Selbstgewählter Name für die Berechtungsgruppen 1 bis 15. Zuweisung von Amtsberechtigungen pro Richtung (Leitungsbündel) jeweils für Tag und Nacht. Bei der Konfiguration der Teilnehmer kann der Zugriff auf externe Rufnummern durch Zuweisung von Berechtigungsgruppen eingeschränkt werden.
Berechtigung	Zuweisen der Berechtigungen zu den einzelnen Berechtigungsgruppen für Nachtbetrieb. Alle Einschränkungen werden nur wirksam an Leitungen einer Richtung des Typs Amt.
Berechtigungsgruppe: Intern	Der Teilnehmer darf nur intern telefonieren. Standardwert: Default in Berechtigungsgruppe 1
Berechtigungsgruppe: Halbamt	Der Teilnehmer darf externe Gespräche nur annehmen. Standardwert: Default in Berechtigungsgruppe 2
Berechtigungsgruppe: Erlaubnisliste	Der Teilnehmer darf nur die in der Erlaubnisliste definierten externen Rufnummern wählen. Ist keine Rufnummer eingetragen gilt Halbamtsberechtigung. Standardwert: Default in Berechtigungsgruppe 4
Berechtigungsgruppe: Verbotsliste	Der Teilnehmer darf die in der Verbotsliste definierten externen Rufnummern nicht wählen. Ist keine Rufnummer eingetragen gilt Vollamtsberechtigung. Standardwert: Default in Berechtigungsgruppe 3, 5, 6
Berechtigungsgruppe: Vollamt	Der Teilnehmer darf ohne Einschränkung kommende und gehende externe Gespräche annehmen und aufbauen. Standardwert: Default in Berechtigungsgruppe 7 bis 15
Gruppenmitglieder anzeigen	Anzeige von Rufnummer und Name der Mitglieder in der ausgewählten Berechtigungsgruppe.

27.3.11.4 Berechtigungen > Erlaubnislisten

Parameterbeschreibung der Registerkarten:

- **Liste anzeigen**
- **Rufnummer hinzufügen**

Parameter	Beschreibung
Liste 1-6	Anzeigen/Hinzufügen/Ändern/Löschen einer erlaubten Rufnummer. Die Erlaubnisliste enthält die Rufnummern, die der Teilnehmer anrufen darf. Es können bis zu 6 Erlaubnislisten erstellt werden. Die 1. Erlaubnisliste kann 100 Einträge enthalten, die übrigen 5 Listen jeweils bis zu 10 Einträge.
Rufnummer	Die einzelnen Rufnummern können bis zu 26 Stellen (Ziffern 0 bis 9 sowie die Zeichen * und #) umfassen. Es muss dabei nicht die vollständige Rufnummer aufgeführt werden. Um Teilnehmer beispielsweise zur Anwahl aller (kostenlosen) 0800xxxer-Nummern zu berechtigen, muss hier lediglich die 0800 eingeben werden. Da sich die Listen nur auf gehende Externgespräche beziehen, muss die Amtsbelegungs-Kennziffer bei den eingetragenen Rufnummern nicht mit angegeben werden.

27.3.11.5 Berechtigungen > Verbotslisten

Parameterbeschreibung der Registerkarten:

- **Liste anzeigen**
- **Rufnummer hinzufügen**
- **Auswertungsfilter ändern**

Parameter	Beschreibung
Liste 1-6	Anzeigen/Hinzufügen/Ändern/Löschen einer verbotenen Rufnummer. Die Verbotsliste enthält die Rufnummern, die der Teilnehmer nicht anrufen kann. Es können bis zu 6 Verbotslisten erstellt werden. Die 1. Verbotsliste kann dabei 50 Einträge enthalten, die übrigen 5 Listen jeweils bis zu 10 Einträge.
Rufnummer	Die einzelnen Rufnummern können bis zu 26 Stellen (Ziffern 0 bis 9 sowie die Zeichen * und #) umfassen. Es muss dabei nicht die vollständige Rufnummer aufgeführt werden. Um beispielweise die Anwahl von (kostenpflichtigen) 0900xxxer-Nummern durch die Teilnehmer zu verhindern, muss hier lediglich die 0900 eingeben werden. Der Eintrag des Zeichens # an erster Stelle einer verbotenen Rufnummer verhindert eine Umgehung der Wahlkontrolle für Systemtelefone, die eine analoge Amtsleitung mit MFV-Wahlverfahren belegen und während der Wahl auf MFV umschalten wollen. Da sich die Listen nur auf gehende Externgespräche beziehen, muss die Amtskennzahl bei den eingetragenen Rufnummern nicht mit angegeben werden.
Auswertungsfilter ändern Über die Auswertungsfilter können Sie zu einer beliebigen Verbotsliste festlegen, welche Ziffern nicht mit der entsprechenden Verbotsliste verglichen werden sollen. Das Kommunikationssystem blendet den eingestellten Ziffernbereich vor der Wahlbewertung aus.	
ab Ziffer ... **bis Ziffer**	In diesem Ziffernbereich (1-25) innerhalb der Rufnummer ist der Auswertungsfilter aktiv.
Zeichen	Durch ein Verbot der Zeichen * und # wird erreicht, dass ein Teilnehmer bei der Eingabe dieser Zeichen die Wahlkontrolle umgehen kann.

27.3.11.6 Berechtigungen > Nachtschaltung

Parameterbeschreibung der Registerkarte:

- **Nachtschaltung ändern**

Parameter	Beschreibung
Berechtigte Teilnehmer für Nachtschaltung	Sollen bestimmte Teilnehmer die Möglichkeit haben, das Kommunikationssystem in den Nachtmodus zu schalten, müssen diese Teilnehmer in die Liste Berechtigte Teilnehmer für Nachtschaltung eingetragen werden. Es können max. 5 Teilnehmer eingetragen werden. Standardwert: 100
Teilnehmer	Liste aller im Kommunikationssystem vorhandenen Teilnehmer.
Berechtigte Teilnehmer	Liste der berechtigten Teilnehmer, die den Nachtmodus aktivieren können.
Hinzufügen >>	Fügt den ausgewählten Teilnehmer zu den berechtigten Teilnehmern hinzu.

27.3.11.7 Berechtigungen > VBZ Gruppenzuordnung

Parameterbeschreibung der Registerkarten:

- **Zuweisung Teilnehmer zu Berechtigungsgruppe ändern**
- **Zuweisung Leitung zu VBZ-Gruppe**
- **Zuweisung KWZ-Bereich zu VBZ-Gruppe**

Parameter	Beschreibung
VBZ Gruppenzuweisung	Zuweisen einer VBZ-Gruppe (1-64) zu einem Teilnehmer Über VBZ-Gruppenzuordnung weisen Sie den einzelnen Teilnehmern des Kommunikationssystems eine VBZ-Gruppe zu. Beim Kodieren der Verbindungsmatrix können Sie dann auf diese Gruppen zurückgreifen und festlegen, welche Teilnehmer welche anderen Teilnehmer erreichen können. Standardmäßig sind alle Teilnehmer der VBZ-Gruppe 1 zugeordnet. Damit haben alle Teilnehmer uneingeschränkten Zugang zu anderen Teilnehmern. Wertebereich: 1 - 64
Zuweisung Leitung zu VBZ-Gruppe	Zuweisen einer Leitung zur VBZ-Gruppe. Über VBZ-Gruppenzuordnung weisen Sie den einzelnen Leitungen des Kommunikationssystems eine VBZ-Gruppe zu. Beim Kodieren der Verbindungsmatrix können Sie dann auf diese Gruppen zurückgreifen und festlegen, welche Teilnehmer auf welche Leitungen zugreifen können. Standardmäßig sind alle Amtsleitungen der VBZ-Gruppe 1 zugeordnet. Damit haben alle Teilnehmer uneingeschränkten Zugang zu Leitungen, sowohl kommend als auch gehend. Wertebereicht: 1 - 64
Zuweisung KWZ-Bereich zu VBZ Gruppe	Jeder VBZ-Gruppe wird ein Bereich von Kurzwahlen (KWZ) zugeordnet. Wählt ein beliebiger Teilnehmer eine KWZ aus, wird durch Bestimmen der dazugehörigen VBZ-Gruppe ermittelt, ob dieser Teilnehmer berechtigt ist, diese KWZ auszuwählen. Liegt diese KWZ im Bereich der zugeordneten KWZ für die entsprechende VBZ-Gruppe, so erfolgt die Wahl. Entspricht die KWZ nicht dem zugeordneten Bereich erfolgt eine Fehlermeldung. Die KWZ-Bereiche können sich in den VBZ-Gruppen überschneiden. Es ist jedoch nicht zulässig, einzelne KWZ in den VBZ-Gruppen und mehrere KWZ-Bereiche in einer VBZ-Gruppe einzutragen. Zulässig sind beispielsweise VBZ 1: 0-99; VBZ 2: 50-150; VBZ 3: 200-500. Nicht zulässig sind beispielsweise VBZ 1: 0, 5, 10; VBZ 2: 50-100, 300-500. Wertebereich: 0-7999

27.3.11.8 Berechtigungen > VBZ Matrix

Parameterbeschreibung der Registerkarten:

- **VBZ-Matrix ändern**

Parameter	Beschreibung
VBZ-Matrix	Wenn Sie eine Verbindungsmöglichkeit zwischen zwei VBZ-Gruppen gezielt bearbeiten möchten, klicken Sie in das Feld am Kreuzungspunkt dieser VBZ-Gruppen in der VBZ-Matrix. Klicken Sie wiederholt in das Feld, um Verbindungsmöglichkeiten in die eine Richtung, in die andere Richtung oder in beide Richtungen freizugeben oder zu sperren. Um die Verbindungsmatrix nutzen zu können, müssen Sie zunächst jeden Teilnehmer über VBZ-Gruppenzuordnung einer Gruppe zuweisen. Bei der Standardeinstellung sind sämtliche Teilnehmer und Leitungen der Gruppe 1 zugeordnet. Nachdem für die Gruppe 1 uneingeschränkter Zugang festgelegt ist, kann bei der Standardeinstellung jeder Teilnehmer auf sämtliche anderen Teilnehmer und Leitungen zugreifen.
Raster	In der Matrix wird eine Liste von Gruppen horizontal am oberen Rand und eine andere Liste vertikal am linken Rand eingeblendet. An den Berührungspunkten befindet sich jeweils ein Kästchen. Der Pfeil in dem betreffenden Kästchen gibt die Beziehung der beiden Gruppen zueinander an. Ein leeres Feld besagt, dass keine Verbindung möglich ist. Eine Verbindungsmatrix, bei der keine Pfeile eingetragen sind, hat eine völlige Blockade des Kommunikationssystems zur Folge.
Alles sperren	Die VBZ-Matrix unterdrückt den Verkehr zwischen Teilnehmern/Leitungen innerhalb einer Gruppe (Teilanlage) und zwischen den Gruppen.
Alles freigeben	Die VBZ-Matrix erlaubt den Verkehr zwischen Teilnehmern/Leitungen innerhalb einer Gruppe (Teilanlage) und zwischen den Gruppen.
Nur guppenintern	Die VBZ-Matrix erlaubt den Verkehr nur zwischen Teilnehmern/Leitungen innerhalb einer Gruppe (Teilanlage).

27.3.11.9 Berechtigungen > Automatische Nachtschaltung

Parameterbeschreibung der Registerkarten:

- **Alle Tage anzeigen**
- **Tag ändern**

Parameter	Beschreibung
Montag, Dienstag, Mittwoch, Donnerstag, Freitag, Samstag, Sonntag, Sondertag	Über den Zeitplan wird die automatische Nachtschaltung eingerichtet. Der Zeitplan umfasst die gesamte Woche (Montag bis Sonntag) sowie Sondertage. Sondertage sind Feiertage oder besondere Tage wie beispielsweise Betriebsferien.
Zone	Der Zeitplan eines Tages kann in bis zu 4 Zonen (Zeitintervalle) unterteilt werden. Die Zonen können lückenlos aufeinander aufsetzen, so kann beispielsweise die Endezeit des ersten Intervalls identisch sein mit der Anfangszeit des zweiten Intervalls. Ein Intervall kann nicht dieselbe Anfangs- und Endezeit haben. Die minimale Länge eines Intervalls beträgt 15 Minuten. Wertebereich: 1-4
Beginn	Anfangszeit für die Zone. Beginnt das erste Intervall eines Tages um 0.00 Uhr, muss die Startzeit als 00:00 eingegeben werden.
Ende	Endezeit für die Zone. Endet das letzte Intervall eines Tages um 24.00 Uhr (12 pm), muss die Endezeit als 23:59 (11:59) eingegeben werden.

Parameter	Beschreibung
Nacht Ruf-Nr.	Nacht-Rufnummer für die Zone. Wird für die Nacht-Rufnummer keine Rufnummer eingetragen, dann greift im System die Nachtschaltung pro Leitung. Die Ziele dafür werden unter Leitungen/Vernetzung > Leitung ändern > Rufzuordnung Ltg eingestellt. Die Zeiten, die über die automatische Nachtschaltung eingetragen werden, gelten für alle Leitungen.
OK	Die Zone wird eingerichtet.
Löschen	Die definierte Zone wird gelöscht.

27.3.11.10 Berechtigungen > Sondertage

Parameterbeschreibung der Registerkarte:

- **Spezielle Tage ändern**

Parameter	Beschreibung
Tag	Bei Auswahl eines Datums im Kalender, wird dieses automatisch hier eingeschrieben.
Name	Name für diesen Sondertag (z. B. Pfingstmontag)

27.3.12 Anschaltungen

Unter **Anschaltungen** sind die Funktionen für die Anschaltungen z. B. für Musik on Hold (MoH) oder für die Anschaltung einer Türsprechstelle/Türöffner an die Anlagen-Ports (Amtsleitungen) zusammengefasst.

27.3.12.1 Anschaltungen > Ansage/Interne Wartemusik > Ansagen und Wartemusik

Parameterbeschreibung der Registerkarten:

- **Ansagen und Wartemusik ändern**

Parameter	Beschreibung
WAV-Datei	Das Eingabeformat für Wartemusik-Dateien ist WAV mit PCM und 16-Bit. Unterstützte Abtastraten: 8 / 22,05 / 24 / 32 / 40 / 44,1 und 48 kHz Mono oder Stereo. Bevorzugtes Format: PCM, 16 Bit, 8 kHz, Mono. Es wird empfohlen, das bevorzugte Eingabeformat zu verwenden und die Länge der WAV-Dateien auf ca. 2 Minuten zu begrenzen. NEU: Je eine MOH für Tag und Nacht! Reset erforderlich!
Zugang	Zugangsaktivierung über Manager E.
Typ	Typaktivierung über Manager E.
Modus	Modusauswahl zum Abspielen der Wartemusik: "Start/Stop" oder "kontinuierlich"

27.3.12.2 Anschaltungen > Türsprechstelle

Parameterbeschreibung der Registerkarten:

- **Türsprechstelle ändern**

Parameter	Beschreibung
Sprechstelle	Auswahl des Rufnummer/Anschlussport der Türsprechstelle. Die Sprechstelle an der Eingangstür muss vom Typ NoFe oder NoPort sein.
Zielstelle	Auswahl der Rufnummer / Anschlussport der Türrufzielstelle. Als Türrufzielstelle, an der nach Betätigung der Türklingel der Ruf signalisiert wird, kann eine Teilnehmerrufnummer oder eine Gruppennummer angegeben werden. Der Ruf folgt den über "Einstellungen - Kommende Rufe" definierten Rufweiterschaltungsalgorithmen.
Türöffner	Freischaltung der Türöffnerfunktion. Ein am TFE-S angeschlossener elektrischer Türöffner wird für die Teilnehmer durch setzten dieses Flag aktiviert.
DTMF	Durch Aktivieren dieses Flags ist die Aktivierung des Türöffners mit einem MFV-Sender von der Ferne aus möglich.
AUL	Durch Aktivieren dieses Flags ist es möglich, die Türrufzielstelle nach extern umzuleiten.

27.3.12.3 Anschaltungen > SmartVM

Parameterbeschreibung der Registerkarten:

- **SmartVM-Mailboxen bearbeiten**

Parameter	Beschreibung
Mailbox-Rufnummer	Eingabe der Mailbox-Rufnummern. Eine Mailbox wird anhand der Mailbox-Rufnummer identifiziert. Wenn eine Mailbox einem Teilnehmer zugeordnet werden soll, ist es zwingend erforderlich, dass die Mailbox dieselbe Rufnummer hat wie der Teilnehmer.
Name	Anzeige des Mailbox-Namens. Der Name entspricht dem Namen des Teilnehmers (falls vorhanden). Bei einer Gruppe wird der Gruppenname angezeigt.
Begrüßung	Auswahl der Begrüßung. Die Nutzbarkeit der angebotenen Einträge ist abhängig vom gewählten Telefonmenü (TUI). Mit der OSO TUI wird für Standardmailboxen nur die Begrüßung 1 unterstützt.
Begrüßung: **Begrüßung 1-4**	Die Auswahl der Begrüßungen 1-4 ist abhängig vom Typ der Mailbox: Standard-Mailbox: Begrüßung 1 oder 2 (mit OSO TUI nur Begrüßung 1) Vermittlungs-Mailbox: Begrüßung 1, 2, 3 oder 4
Begrüßung: **Tag/Nacht**	Begrüßung ist abhängig vom Tag-/Nachtbetrieb: Tag - Begrüßung 1 / Nacht - Begrüßung 2
Begrüßung: **Typ of Call**	nur für Standard-Mailbox: Begrüßung ist abhängig von dem Zustand des Teilnehmers: Anruf nicht angenommen - Begrüßung 1 / Besetzt - Begrüßung 2
Begrüßung: **Kein**	Es wird keine Begrüßung abgespielt. Die Mailbox bleibt aber aktiv, z. B. für eine Weiterleitung des Anrufs zum Abwurfplatz.

Parameter	Beschreibung
Aufnahme	Ist dieses Flag aktiviert, ist die Mailbox eine Standard-Mailbox. Sie kann dann keine Vermittlungs-Mailbox mehr sein. Ist das Flag deaktiviert (Standard), hat die Mailbox nicht die Möglichkeit, eine Nachricht aufzusprechen. Der Teilnehmer kann eim ersten Abfragen seiner Mailbox die Aufnahme aktivieren. Dadurch ist gewährleistet, dass vor der Erstinbetriebnahme durch den Teilnehmer keine Nachrichten aufgezeichnet werden können. Standard: Aktiviert
AutoAttendant	Ist dieses Flag aktiviert, ist die Mailbox eine Vermittlungs-Mailbox (AutoAttendant). Sie kann dann keine Standard-Mailbox mehr sein. Es können maximal 100 Mailboxen als Vermittlungs-Mailboxen eingerichtet werden. Beim Wechseln einer Standard-Mailbox auf eine Vermittlungs-Mailbox werden alle Nachrichten der Mailbox gelöscht. Standard: Deaktiviert
Passwort Reset	Ist dieses Flag aktiviert, wird das Passwort der Mailbox auf `123456` zurückgesetzt. Der Teilnehmer muss das Passwort beim nächsten Zugriff auf seine Mailbox ändern. Standard: Deaktiviert

Parameterbeschreibung der Registerkarten:

- **SmartVM-Parameter bearbeiten**

Parameter	Beschreibung
allgemeine Parameter	
maximale Mailbox-Nummernlänge	Maximale Länge der Mailbox-Rufnummer. Wertebereich: 2 - 16 Stellen, Standardwert: 3 Stellen
Max. Nachrichtenlänge (Min.)	Maximale Länge der Aufnahmedauer einer Nachricht. Wertebereich: 1 oder 2 Minuten, Standardwert: 2 Minuten
Rufnummernlängenbegrenzung	Bei gehenden Verbindungen, die von der SmartVM eingeleitet werden (AutoAttendant Nachwahl und AutoAttendant Kurzwahl) können nur Rufnummern bis zur angegebenen Länge gewählt werden. Bei eingerichteten längeren Rufnummern unterbleibt der Verbindungsaufbau. Im Standard entspricht die Rufnummernlängenbegrenzung der Mailbox-Rufnummernlänge (interne Rufnummernlänge), so dass nur eine Internwahl erlaubt ist. Wertebereich: 2- 30, Standardwert: 3
Allgemeines Fax-Abwurfziel	Eingabe des Fax-Abwurfziels, auf das die SmartVM normalerweise ankommende Faxe schicken soll. Ist kein Fax-Abwurfziel angegeben, werden ankommende Faxe abgewiesen. Wertebereich: max. 16 Ziffern
Standardsprache	Auswahl der Sprache der Benutzerführung. Gilt für alle Mailboxen. Ist die Benutzerführung in der gewünschten Sprache nicht vorhanden, wird die Sprache auf UK-Englisch (enuk) gesetzt.
Telephone User Interface (TUI)	Auswahl der Telefonmenüstruktur der Sprachbox (Telefone User Interface, TUI). Die Auswahl gilt für alle Mailboxen.
Telephone User Interface (TUI): **SmartVM**	SmartVM TUI, ähnlich zur Xpressions Compact / EVM TUI (Standard).
Telephone User Interface (TUI): **OSO**	OSO TUI, ähnlich zur UC Suite TUI.

Parameter	Beschreibung
Reihenfolge der Datumsansage	nur sichtbar mit SmartVM TUI: Einstellung der Ansagenreihenfolge für Nachricht, Aufnahmedatum und Rufnummer des Anrufer (falls bekannt).
Reihenfolge der Datumsansage: **Datum nach Nachricht**	nur sichtbar mit SmartVM TUI: Nachricht -- Aufnahmedatum -- Rufnummer des Anrufers (falls bekannt).
Reihenfolge der Datumsansage: **Datum vor Nachricht**	nur sichtbar mit SmartVM TUI: Aufnahmedatum -- Rufnummer des Anrufer (falls bekannt) -- Nachricht. Für Nachrichten von internen Teilnehmern gilt: Name des internen Teilnehmers (falls vorhanden) -- Aufnahmedatum -- Rufnummer des Anrufers (falls bekannt) -- Nachricht.
Anzahl der Nachrichten pro Mailbox	Maximale Anzahl der Nachrichten für eine Mailbox. Wertebereich: 0 - 100, Standardwert: 30
EVM deaktivieren	Ist dieses Flag aktiviert, ist die SmartVM deaktiviert. Standard: Deaktiviert
AA-VP-Verhalten Einstellung, ob der AutoAttendant für bestimmte Fälle automatisch Ansagen abspielen soll.	
VP vor Übergabe	Ist dieses Flag aktiviert, wird im Fall "VP vor Übergabe" folgende Ansage abgespielt: „Bitte warten, Sie werden verbunden...“ Standard: Deaktiviert
VP-Übergabe-Ergebnis	Ist dieses Flag aktiviert, wird im Fall "VP-Übergabe-Ergebnis" eine der folgenden Ansagen abgespielt: „Die Teilnehmernummer existiert nicht.“ „Der Teilnehmer ist besetzt.“ „Der Teilnehmer antwortet nicht.“ Standard: Deaktiviert
VP-Abwurf	Ist dieses Flag aktiviert, wird im Fall "VP-Abwurf" eine der folgenden Ansagen abgespielt: „Sie werden mit dem Operator verbunden. Bitte warten Sie.“ „Sie werden mit der Mailbox des Teilnehmers verbunden.“ „Bitte warten, Sie werden verbunden...“ Standard: Deaktiviert
VP vor Trennen	Ist dieses Flag aktiviert, wird im Fall "VP vor Trennen" eine der folgenden Ansagen abgespielt: „Bitte rufen Sie später an.“ „Vielen Dank. Auf Wiedersehen.“ „Die Mailboxnummer ist ungültig.“ Standard: Aktiviert

Parameterbeschreibung der Registerkarten:

- **AutoAttendant-Parameter bearbeiten**

Parameter	Beschreibung
Rufnummer	Rufnummer des AutoAttendants (Standard 352).
Abwurf nach Ansage	Ist dieses Flag aktiviert, erfolgt nach der Begrüßungsansage der Abwurf des Anrufs zum Abwurfplatz (z. B. Vermittlungsplatz). Während der Begrüßungsansage ist es nicht möglich ein Kurzwahlziel anzuwählen. Standard: Deaktiviert
keine Nachwahl	Ist dieses Flag aktiviert, kann der Anrufer nur über die Wahl der Kurzwahlziele zu anderen Zielen weitergeleitet werden. Der Anrufer kann keine mehrstellige Rufnummer wählen. Standard: Deaktiviert

Parameterbeschreibung der Registerkarten:

- **Kurzwahl-/Abwurfziel (Tag) bearbeiten**
- **Kurzwahl-/Abwurfziel (Nacht) bearbeiten**
- **Kurzwahl-/Abwurfziel 3 bearbeiten**
- **Kurzwahl-/Abwurfziel 4 bearbeiten**

Parameter	Beschreibung
Auswählen	Auswahl eines internen Teilnehmers (1. Hälfte der Liste) oder einer Sprachbox (2. Hälfte der Liste) als Kurzwahlziel oder Abwurfplatz.
Aktion	Anzeige der 10 möglichen Kurzwahlziele und des Abwurfplatzes.
Rufnummer	Rufnummer des ausgewählten Teilnehmers oder der ausgewählten Sprachbox.
Name	Name des ausgewählten Teilnehmers oder der ausgewählten Sprachbox.
Typ	Auswahl des Typs der Rufnummer.
Typ: **Rufnummer**	Hier wird mit der zugeordneten Kurzwahlziffer der ausgewählte Teilnehmer angerufen.
Typ: **Mailbox**	Hier wird mit der zugeordneten Kurzwahlziffer die ausgewählte Sprachbox angerufen.

27.3.13 Payload

Unter **Payload** sind die Funktionen für Anzeige und Konfiguration von Anschlusstypen und Protokollen zusammengefasst.

27.3.13.1 Payload > Devices

Parameterbeschreibung der Registerkarten:

- **Globale Device-Einstellungen anzeigen**
- **Device-Einstellungen auf Lieferzustand zurücksetzen**

Parameter	Beschreibung
Globales Gateway vom Typ G.711	Devices ist der Sammelbegriff für Teilnehmer, Leistungsmerkmale und Funktionen, die Kanäle benötigen. Es werden der Codec-Typ des globalen Gateways, die maximale Anzahl verfügbarer und lizenzierter B-Kanäle, sowie die maximale Anzahl von LAN-Clients an einem Kanal für Music on Hold (überzählige Anrufe werden nicht durchgeschaltet) angezeigt.
Max. Anz. von B-Kanälen der HW	
Anz. LAN-Clients an einem MoH-Kanal	

Das Rücksetzen der Device-Einstellungen erfordert einen Restart des Kommunikationssystems.

27.3.13.2 Payload > Media Stream Control (MSC)

Parameterbeschreibung der Registerkarten:

- **MSC-Jitter-Parameter ändern**

Parameter	Beschreibung
	Die Medienstromsteuerung (MSC) überwacht und verwaltet die Medienströme, die durch das Kommunikationssystem geleitet werden. Sie sorgt für die Übermittlung von Mediendaten zwischen Netzen über Gateways (TDM/IP).
Verkehrsstatistik (nur SNMP)	Erforderlich für Zugang zu den Daten der Per-Call-Statistik des Systems über SNMP.
Intervall für Generierung von RTCP-Paketen (sec.)	Reportintervall in Sekunden für RTCP-Pakete (Real-time Transport Control Protocol) zur Aushandlung und Einhaltung von Quality of Service (QoS) Parametern durch den periodischen Austausch von Steuernachrichten zwischen Sender und Empfänger. Wertebereich: 5 bis 10, Standardwert: 5

Parameterbeschreibung der Registerkarten:

- **MSC-Einstellungen auf Lieferzustand zurücksetzen**

Parameter	Beschreibung
MSC-Einstellungen auf Lieferzustand zurücksetzen	Wiederherstellen aller ursprünglichen MSC-Einstellungen.

27.3.13.3 Payload > HW-Module

Verwaltung der DSP-Module des Kommunikationssystems

Parameterbeschreibung der Registerkarten:

- **Alle HW-Module anzeigen**
- **DSP-Einstellungen ändern**
- **DSP Jitter-Einstellungen ändern**

Parameter	Beschreibung
HW-Typ	Anzeige der im Kommunikationssystem verwendeten DSPs (Digital Signal Processor). Möglich sind: • **Onboard** = Integrierter DSP des Mainboards • **OCCB X-1** = DSP eines OCCB-Submoduls (OCCB1 oder OCCB3)
Firmware-Version	Aktuelle Firmware-Version jedes einzelnen DSPs
API-Version	Aktuelle API (Application Programming Interface)-Version jedes einzelnen DSPs
Allgemein	
IP- Adresse	IP-Adresse des DSP-Moduls (Änderbar, falls die IP-Adresse bereits vergeben ist.)
Port	Portnummer des DSP-Moduls
Statusanzeige	Dient zur Erkennung der Verfügbarkeit der DSPs Standardwert: Status messages
Echokompensationsglied	Bei aktiviertem Flag wird die Audio-Rückkopplung (Echo-Effekt) bei Sprachübertragungen unterdrückt. Standardwert: Aktiviert
MFV-Außerband-Signalisierung	Bei aktiviertem Flag werden MFV-Signale im separaten Signalisierungskanal (Outband) übertragen. Standardwert: Deaktiviert
Fax-Parameter	
Fehler-Korrektur-Modus	Bei aktiviertem Flag wird die Fehlerkorrektur während der Übertragung durchgeführt (Error Correction Mode im T.30-Protokoll). Die eingesetzten Faxgeräte müssen diesen Modus ebenfalls unterstützen. Standardwert: Aktiviert
Anzahl redundanter Pakete	Definition der Anzahl der Redundanz-Pakete: Je größer dieser Wert ist, desto robuster ist die Faxübertragung gegenüber Paketverlusten. Nachteil bei größeren Werten ist der Anstieg der benötigten Bandbreite. Standardwert: 2
Maximaler Netzwerk-Jitter (hex ms)	Definition des maximalen Netzwerk-Jitters in Millisekunden: Je größer der Wert ist, desto größer ist die mögliche Laufzeit-Varianz von Datenpaketen in Netzwerken. Erlaubt sind ausschließlich hexadezimale Werte, bestehend aus den Ziffern 0 bis 9 und A bis F. An diesem Parameter sollten möglichst keine Änderungen vorgenommen werden. Standardwert: 00C8
Timeout für Fax/Modem-Ton-Erkennung (s)	Definition der Zeit in Sekunden für die Erkennung von Faxtönen während einer Verbindung: Hierdurch ist eine Umschaltung auf das Faxprotokoll T.38 gewährleistet. Nach Ablauf der hier eingestellten Zeit werden keine Faxtöne mehr erkannt. Der Wert 0 bedeutet, dass die Tonerkennung für die gesamte Dauer der Verbindung aktiviert ist. Standardwert: 0
DSP Jitter	
Jitter-Buffer-Typ	Definition des Jitter-Buffer-Typs Standardwert: Adaptiv
Jitter-Buffer-Typ: Statisch	Die Durchschnittsverzögerung des Jitter-Buffers bleibt stets gleich.

Parameter	Beschreibung
Jitter-Buffer-Typ: Adaptiv	Der Jitter-Buffer passt die Durchschnittsverzögerung an die Situation beim Datenempfang an. Dabei wird versucht, die Verzögerung so gering wie möglich zu halten und zugleich so wenige Datenpakete wie möglich zu verlieren.
Durchschnittl. Verzögerung für Sprache (ms)	Definition der Zeit in Millisekunden, die ein Paket bei IP-basierten Sprachübertragungen durchschnittlich im Jitter-Buffer gehalten werden soll. ***INFO:*** Beim **Jitter-Buffer-Typ Adaptiv** stellt der hier definierte Wert lediglich einen Anfangswert dar. Standardwert: 40
Max. Verzögerung für Sprache (ms)	Definition der maximalen Zeit in Millisekunden für die Verzögerung für Sprache **Jitter-Buffer-Typ Statisch**: Anzugeben ist, wie viele Millisekunden eine tatsächlich gemessene Verzögerung beim Eintreffen von IP-Paketen bei Sprachübertragung betragen darf, bevor der Jitter-Buffer regulierend in den Datenstrom eingreift. Bei statischem Jitter-Buffer ist 80 ein für die meisten Umgebungen empfehlenswerter Wert. **Jitter-Buffer-Typ Adaptiv**: Anzugeben ist, wie viele Millisekunden die Durchschnittsverzögerung für Sprache maximal betragen darf. Ist die tatsächlich gemessene Verzögerung größer, gehen Pakete verloren. Bei adaptivem Jitter-Buffer ist 120 ein für die meisten Umgebungen empfehlenswerter Wert. ***HINWEIS:*** Der Wert muss in jedem Fall größer sein, als der im Feld Durchschnittl. Verzögerung für Sprache (ms) eingetragen ist. Standardwert: 120
Min. Verzögerung für Sprache (ms)	Definition der minimalen Zeit in Millisekunden für die Verzögerung für Sprache **Jitter-Buffer-Typ Adaptiv**: Anzugeben ist, wie viele Millisekunden die Durchschnittsverzögerung für Sprache minimal betragen darf. Die Durchschnittsverzögerung wird in jedem Fall größer oder gleich sein als dieser Wert. Standardwert: 20

Parameter	Beschreibung
Paket-Verlust / Verzögerungpräferenz	Definiert wird das Verhältnis Paketverlust zu Laufzeitverzögerungen von Datenpaketen **Jitter-Buffer-Typ Adaptiv**: Anzugeben ist ein Wert zwischen 0 und 8. Der Wert ist abhängig davon, ob im Fall von großen Laufzeitverzögerungen eher der Verlust von Paketen in Kauf genommen werden kann oder eher eine noch größere Verzögerung. Der Wert 0 bedeutet minimalen Paketverlust mit dem Nachteil von Laufzeitverzögerungen. Der Wert 8 bedeutet minimale Laufzeitverzögerung mit dem Nachteil von möglichen Paketverlusten. Ein für die meisten Umgebungen empfehlenswerter Wert ist 4. Standardwert: 4
Durchschnittl. Verzögerung für Daten (ms)	Definition der durchschnittlichen Verzögerung für Daten in Millisekunden Anzugeben ist, wie viele Millisekunden ein Datenpaket bei Datenübertragungen durchschnittlich im Jitter-Buffer gehalten werden soll. Ein für die meisten Umgebungen empfehlenswerter Wert ist 60. Standardwert: 60
Max. Verzögerung für Daten (ms)	Definition der maximalen Verzögerung für Daten in Millisekunden Anzugeben ist, wie viele Millisekunden eine tatsächlich gemessene Verzögerung beim Eintreffen von IP-Paketen betragen darf, bevor der Jitter-Buffer regulierend eingreift. Ein für die meisten Umgebungen empfehlenswerter Wert ist 200. ***INFO:*** Größere Werte (ab ca. 2000) haben keinen Einfluss. Sobald ein Paket im Puffer komplett empfangen wurde, verlässt dieses Paket den Puffer auch wieder. Werte unter 100 ms sind zwar möglich, aber in der Praxis auf keinen Fall zu empfehlen. Standardwert: 200

27.3.14 Statistiken

Unter **Statistiken** sind die Funktionen für die Anzeige von Statistiken zusammengefasst.

27.3.14.1 Statistiken > Gateway-Statistk > Mainboard > Device-Statistiken

Parameterbeschreibung der Registerkarten:

- **SCN-Statistik anzeigen**
- **LAN-Statistik anzeigen**

Parameter	Beschreibung
Device-Typ	Anzeige der vorhandenen LAN- und SCN (Switched Circuit Network) - Komponenten.
Aktuell belegte Ressourcen	Anzeige der aktuell belegten Ressourcen einer Komponente (konfigurierte und verwendete Kanäle).

Parameter	Beschreibung
Summe	Anzeige der Summe der aktuell belegten Ressourcen.
Autom. Aktualisierung	Die Anzeige wird automatisch alle 60 Sekunden aktualisiert.
Sekunden bis zur nächsten Aktualisierung	Anzeige eines rückläufigen Timers, beginnend bei 60 Sekunden.

27.3.14.2 Statistiken > Gateway-Statistken > Mainboard > MSC-Statistiken

Parameterbeschreibung der Registerkarten:

- **Gesamt-Statistik anzeigen**
  MSC-Statistiken sind Statistiken des Medienstroms, der über digitale Signalprozessoren zwischen IP und TDM umgesetzt wird (Media Stream Control). Die MSC-Gesamt-Statistik bietet einen Überblick über die statistischen Daten für alle registrierten Gespräche. Sie gibt Aufschluss über gesendete und nicht gesendete RTP/TCP-Pakete, über empfangene und nicht empfangene Pakete und über die Anzahl gesendeter und empfangener Bytes.

Parameterbeschreibung der Registerkarten:

- **Einzelruf-Statistik anzeigen**
  Die MSC-Einzelruf-Statistik listet tabellarisch für jede Verbindung mit Umsetzung über digitale Signalprozessoren die Verbindungsdaten und verwendete Parameter auf. Sie dient Experten zur Fehleranalyse.

27.3.14.3 Statistiken > SNMP Statistik

Parameterbeschreibung der Registerkarten:

- **Statistik-Tabelle anzeigen**
- **Statistik anzeigen**

Parameter	Beschreibung
if-Tabellen-Statistik	In SNMP erfasste Details zu einzelnen Schnittstellen (if = Interface) im Kommunikationssystem, wie zum Beispiel Ethernet-Schnittstellen.
IP-Statistik	Details und Fehler zum IP-Routing
TCP-Statistik	Details und Fehler zum TCP-Protokoll
UDP-Statistik	Details und Fehler zum UDP-Protokoll

27.3.14.4 Statistiken > Telephonie Statistiken > System Texte

Parameterbeschreibung der Registerkarten:

- **Display System Texts**

Parameter	Beschreibung
Verfügbare Sprachen	Anzeige der im Kommunikationssystem verfügbaren Sprachen für die Telefon-Displays

27.3.14.5 Statistiken > Telephonie Statistiken > UCD Agenten

Parameterbeschreibung der Registerkarten:

- **UCD Agenten anzeigen**

Parameter	Beschreibung
Anzahl UCD Agenten	
Gesamt	Gesamtzahl der im Kommunikationssystem angemeldeten UCD-Agenten
Verfügbar	Anzahl der verfügbaren UCD-Agenten
UCD Agenten Status	
Rufnummer	Rufnummer des UCD-Agenten
Name	Name des UCD-Agenten
ID	ID des UCD-Agenten
UCD-Gruppe	UCD-Gruppe, der der UCD-Agent zugeordnet ist.
Status	Status des UCD-Agenten

27.3.14.6 Statistiken > Telephonie Statistiken > Zustand Leitung

Parameterbeschreibung der Registerkarten:

- **Leitungsstatus anzeigen**

Parameter	Beschreibung
Datum	Datum der Statusabfrage bzw. der letzten Statusänderung der Leitung
Uhrzeit	Uhrzeit der Statusabfrage bzw. der letzten Statusänderung der Leitung
Slot/Port	Anzeige der Baugruppe, des Einbauplatzes (Slot) und der Schnittstelle (Port) bzw. der LAN-Schnittstelle
Trunk Number	Leitungskennzahl
Kommentar	Status der Leitung (Angezeigt wird der letzte Zustand der Leitung.) Möglich sind folgende Leitungszustände: • **Idle** (Leitung im Ruhezustand) • **Alerting** (Ruf steht an) • **Connected to:** (Verbindung zur angezeigten Rufnummer) • **Leitung gesperrt** • **Leitung ausgefallen**

27.3.14.7 Statistiken > Telephonie Statistiken > Weiterleitung

Parameterbeschreibung der Registerkarten:

- **Weiterleitungen anzeigen**

Parameter	Beschreibung
Anrufumleitung	
Status	Status der Anrufumleitung: • **aus** (keine Anrufumleitung aktiv) • Bei aktiver Anrufumleitung werden Art der Anrufumleitung und Umleitungsziel angezeigt.
Umleitungsziel von	Anzeige, ob der Teilnehmer das Umleitungsziel der Anrufumleitung eines anderen Teilnehmers ist. Angezeigt werden Rufnummer und Name des umleitenden Teilnehmers.
Rufzuschaltung ein	
Zugeschaltete Teilnehmer	Rufnummer und Name von zugeschalteten Teilnehmern
Zuschaltung von	Anzeige, ob der Teilnehmer das Rufzuschaltungsziel eines anderen Teilnehmers ist. Angezeigt werden Rufnummer und Name des rufzuschaltenden Teilnehmers.

27.3.14.8 Statistiken > Telephonie Statistiken > Teilnehmer

Parameterbeschreibung der Registerkarten:

- **Teilnehmer Parameter anzeigen**
- **Aktivierte Merkmale anzeigen**

Parameter	Beschreibung
Rufnummer	Rufnummer des Teilnehmers
Name	Name des Teilnehmers
Durchwahl	Durchwahlnummer des Teilnehmers
Endgeräte Typ	Typ des Telefons, wie zum Beispiel OpenStage 60
Clip/Lin	Location Identification Number LIN Nur für USA, Kanada: Durch den erweiterten Notrufdienst E911 werden neben der Rufnummer auch Informationen über den geographischen Standort des Anrufers beim Absetzen eines Notrufs übermittelt. Dazu wird jedem Teilnehmeranschluss mit gültiger Durchwahlnummer eine LIN zugeordnet.
Access	Bei analogen und $U_{P0/E}$-Telefonen Anzeige der Baugruppe, des Einbauplatzes und der Nummer des Anschlusses. Zusätzliche Anzeige bei $U_{P0/E}$-Telefonen, ob Master oder Slave. Bei IP-Telefonen Anzeige der LAN-Schnittstelle, des Typs und der Nummer
Parameter	
Stationstyp	Stationstyp, wie zum Beispiel Standard oder Fax Standardwert: Standard

Parameter	Beschreibung
Sprache	Spracheinstellung des Telefons
Rufsignalisierung intern	Rufart für die Signalisierung interner Anrufe Standardwert: Rufart 1
Rufsignalisierung extern	Rufart für die Signalisierung externer Anrufe Standardwert: Rufart 1
Berechtigung (LCR)	Berechtigungsklasse des Teilnehmers für Least Cost Routing Standardwert: 15
Lizenz Typ	Lizenztyp des Teilnehmers
Merkmale	
Anrufschutz	Status des Leistungsmerkmals Anrufschutz Standardwert: Aus
Antworttext	Status des Leistungsmerkmals Antworttext Standardwert: Aus
Codeschloss	Status des Leistungsmerkmals Codeschloss Standardwert: Aus
Rufnummerunterdrückung	Status des Leistungsmerkmals Rufnummerunterdrückung Standardwert: Aus
Rufzuschaltung	Status des Leistungsmerkmals Rufzuschaltung Standardwert: Aus
Ruhe schalten	Status des Leistungsmerkmals Stiller Ruf/Ruhe Standardwert: Aus
Sammelanschluss/Gruppe	Status des Leistungsmerkmals Sammelanschluss/Gruppenruf Standardwert: Aus
Stilles Anklopfen	Status des Leistungsmerkmals Stilles Anklopfen Standardwert: Aus
Direktantworten	Status des Leistungsmerkmals Direktantworten Standardwert: Aus
Freigeben zum Anklopfen	Status des Leistungsmerkmals Freigeben zum Anklopfen Standardwert: Aus
Umleitung nach Zeit	Status des Leistungsmerkmals Umleitung nach Zeit Standardwert: Aus
AUL	Status des Leistungsmerkmals Anrufumleitung (AUL) Standardwert: Aus

27.4 Applikationen

Unter **Applikationen** sind Funktionen für die Konfiguration des Application Servers für Unified Communications un der Web Services zusammengefasst.

27.4.1 Applikationsauswahl

Unter **Applikationsauswahl** sind Funktionen für die Auswahl der verwendeten Lösung für Unified Communications zusammengefasst.

27.4.1.1 Applikationsauswahl

Parameterbeschreibung der Registerkarten:

- **Applikationsauswahl**

Parameter	Beschreibung
Applikationspakete auswählen	Auswahl der Applikationspakete mit UC Smart oder mit UC Suite. Bei dem Applikationspaket mit UC Suite auf dem OpenScape Business UC Booster Server wird zusätzlich die IP-Adresse des UC Booster Servers (IP-Adresse des Linux-Servers) benötigt.
Applikationsauswahl	Anzeige der unterstützten Komponenten je nach ausgewähltem Applikationspaket inkl. der IP-Adresse des verwendeten Servers.

27.4.2 UC Smart

Unter **UC Smart** sind Funktionen von Unified Communications zusammengefasst.

27.4.2.1 UC Smart > Grundeinstellungen

Parameterbeschreibung der Registerkarten:

- **Grundeinstellungen**

Parameter	Beschreibung
Sicherheit	
UC Smart Aktivieren/Deaktivieren	
Aktiv	UC Smart und UC Suite können nicht gleichzeitig aktiv sein. (Nach Aktivieren werden weitere Parameter angezeigt)
Zugangseinstellungen	

Parameter	Beschreibung
HTTP	UC Smart Clients können grundsätzlich über HTTPS verschlüsselt (empfohlen) oder HTTP unverschlüsselt (nicht empfohlen) auf das System zugreifen. Die Auswahl wird in der Applikation selbst getroffen. Hier wird die Berechtigung für eines oder beide Protokolle erteilt.
HTTPS	
Passwort-Policy	
Benutzer muss sicheres Passwort eingeben	Kennwort-Richtlinie für UC Smart Clients. Das standardmäßige Kennwort muss bei der ersten Anmeldung geändert werden und dabei der hier gewählten Richtlinie entsprechen (siehe Fragezeichen-Schaltfläche). Das Kennwort wird im Client gespeichert, ansonsten wird es bei jedem beim Start des Clients abgefragt.
Anmeldedaten im Endgerät speichern	Die Anmeldedaten werden zusätzlich im Telefon gespeichert.
Systemweites initiales UC Smart Passwort	Ein systemweites initiales Passwort wirkt sich auf alle konfigurierten UC Smart User aus, die sich noch nie in UC Smart eingeloggt haben bzw. die noch nicht ihr initiales Passwort geändert haben. Jeder betroffene User muss anschließend ein individuelles Passwort vergeben. ***INFO***: die Vergabe eines systemweiten initialen UC Smart Passwortes stellt ein Sicherheitsrisiko dar, insbesondere wenn einzelne User nicht zeitnah ein persönliches Passwort vergeben. Alternativ empfiehlt sich die Vergabe individueller initialer Passwörter für jeden User.

27.4.2.2 UC Smart > Benutzerverwaltung

Parameterbeschreibung der Registerkarten:

- **Benutzerverwaltung**

Parameter	Beschreibung
Benutzer	Liste aller vorhandenen Teilnehmer, der ausgewählte Teilnehmer muss eine UC Smart Lizenz erhalten
Einstellungen	
Benutzer	Anzeige der internen Telefonnummer des Benutzers.
Name	Anzeige des Namens des Benutzers.
Passwort	Kennwort des Benutzers des UC Smart Clients kann hier festgelegt werden.
Sprache	Sprache von UC Smart Assistant
Anwender muss neues Passwort vergeben	(nur Anzeige)
Zugriff auf UC Smart Assistant	Berechtigung für Zugriff auf UC Smart Assistant durch den Benutzer
Konfiguriert als Mobility-Teilnehmer	(nur Anzeige)
Voicemail-Lizenz	(nur Anzeige)
Assoziierte Dienste	(nur Anzeige)
Profildetails	

Parameter	Beschreibung
Mobile Rufnummer	Mobile Rufnummer des Teilnehmers im kanonischen Format (z. B. `+49 173 1234567`).
Private/Externe Rufnummer	Zusätzliche Rufnummer des Teilnehmers im kanonischen Format (z. B. `+49 89 987654321`).
Email-Adresse	E-Mail-Adresse des Teilnehmers.
Voicemail an Email	Aktivierung/Deaktivierung der Email-Benachrichtigung beim Eingang einer neuen Sprachnachricht.
Sichtbarkeit Präsenzstatus	Einstellung, ob der Anwesenheitsstatus für interne und externe Teilnehmer sichtbar sein soll oder nur für interne Teilnehmer oder ob er überhaupt nicht sichtbar sein soll.
Lizenzierungsinformationen	Anzeige der im System vorhandenen Lizenzen für die jeweilige Applikation

27.4.2.3 UC Smart > Status

Parameterbeschreibung der Registerkarten:

- **Status**

Parameter	Beschreibung
Applikationsserver	Anzeige des Status des integrierten UC Smart Applikationsservers.
Aktive Verbindungen	Anzeige der Anzahl der aktiven Verbindungen pro UC Smart Client.

27.4.3 OpenScape Business UC Suite

Unter **OpenScape Business UC Suite** sind Funktionen von Unified Communications zusammengefasst, wie z. B. Konferenzschaltung, Abteilungen und Gruppen, Konfiguration des externen Verzeichnisses, Urlaubs- und Zeitpläne, das Contact Center und die Server-Einstellungen für UC Suite.

27.4.3.1 OpenScape Business UC Suite

Parameter	Beschreibung
OpenScape Business UC Suite	Konfiguration von UC Suite, inkl. der Clients myPortal, myAgent, myAttendant und myReports, Sprach- und Faxnachrichten sowie Konferenzen.

27.4.3.2 OpenScape Business UC Suite > Benutzerverzeichnis

Parameter	Beschreibung
Symbol für Anwesenheitsstatus	Der Administrator kann den Anwesenheitsstatus für jeden Benutzer ändern. Eine graue Figur ist momentan nicht an UC Suite angemeldet.
Bearbeiten	Einstellungen des ausgewählten UC Suite Benutzers bearbeiten
Benutzer zurücksetzen	Die Einstellungen eines Benutzers werden auf Standardwerte zurückgesetzt. Dabei werden seine Sprachnachrichten, persönliche Ansagen der Sprachbox, Journaleinträge, geplante Konferenzen, E-Mails und Faxnachrichten gelöscht.
Benutzer entsperren	Gesperrte Benutzer (z. B. nach mehrfach falscher Passworteingabe) können hier entsperrt werden, Anzeige Schloss-Symbol. Der Administrator kann vom System via Email über die Sperrung informiert werden.
Persönliche Daten	Persönliche Daten des Benutzers
Persönliche Daten: Eigene persönliche Daten	Eigener Name, Benutzername, Kennwort, E-Mail-Adresse, Abteilung, Zusätzliche Rufnummer (kanonisches Format, z. B.+49 89 700798765), XMPP-ID. Das Kennwort gilt für UC Suite Clients.
Persönliche Daten: Eigenes Bild	Wird automatisch skaliert
Persönliche Daten: Benutzerebene	Nur vom Administrator für Contact Center einstellbar: Wenn der Agent dauerverfügbar sein soll, aktivieren Sie das Kontrollkästchen **Dauerverfügbarer Agent**. Der Agent bleibt auch dann für Anrufe, Faxe und E-Mails verfügbar, wenn er einen Anruf, ein Fax oder eine E-Mail nicht angenommen hat. Bei der Konfiguration eines Teilnehmers als Agent werden die Rechte des Agenten durch Auswahl des Berechtigungs-Levels definiert (Agent, Supervisor oder Administrator). Ein Agent mit dem Berechtigungs-Level Supervisor oder Administrator verfügt über erweiterte Berechtigungen.
Meine Einstellungen	Benutzerspezifische Einstellungen des Clients
Meine Einstellungen: Darstellung	Skin-Farben der Benutzeroberfläche, Sprache der Benutzeroberfäche
Meine Einstellungen: Benachrichtigungen	Einstellungen für das PopUp-Fenster
Meine Einstellungen: Outlook-Anbindung	Kalendertermine generieren: Übernahme des Anwesenheitsstatus in den Outlook-Kalender Kalenderintegration: Steuerung des Anwesenheitsstatus durch Outlook-/iCal-Termine (erstes Schlüsselwort in der Betreffzeile steuert Anwesenheitsstatus)
Meine Einstellungen: Abkürzungstasten	Definition von Tastenkombinationen für Anruffunktionen
Meine Einstellungen: Verschiedenes	Automatisches Zurücksetzen des Anwesenheitsstatus nach Terminende auf Status "Büro", Aufzeichnuung von Client-Logs aktivieren, Festlegung der Übergabemethode, Aufbewahrungsdauer für Journaleinträge (Maximalwert ist unter Server > Wartung > Anrufhistorie), Programmierung von Funktionstasten des Telefons
Anrufregeln	Regeln für kommende Rufe
Anrufregeln: Anrufweiterleitungsziele	Festlegung der Weiterleitungsziele für jeden Anwesenheitsstatus (statusbezogene Anrufumleitung)
Anrufregeln: Regelmodul	Festlegung komplexer Anrufregeln in Abhängigkeit vom Anwesenheitsstatus (regelbasierte Anrufumleitung)
Kommunikation	Behandlung der benutzerspezifischen Nachrichten

Parameter	Beschreibung
Kommunikation: Einstellungen für Sprachnachrichten	Aufzeichnung von Sprachnachrichten im jeweiligen Anwesenheitsstatus ist möglich; Einstellung der Voicemail-Sprache Standardwert: deaktiviert
Kommunikation: Sprachnachricht-Benachrichtigung	Benachrichtigungsdienst für neue Sprachnachrichten - E-Mail-Adresse siehe Eigene persönliche Daten, Voraussetzung: Mailserver und eigene Mailadresse ist unter Servicecenter > Email-Weiterleitung konfiguriert - "Gehend" erzeugt einen User-Outcall zur angebenen Rufnummer (kanonisches Format) - SMS-Rufnummer siehe Eigene persönliche Daten, Inhalt der SMS siehe Templates
Kommunikation: Fax-Benachrichtigung	Benachrichtigungsdienst für neue Faxnachrichten - E-Mail-Adresse siehe Eigene persönliche Daten, Voraussetzung: Mailserver und eigene Mailadresse ist unter Servicecenter > Email-Weiterleitung konfiguriert - "Gehend" erzeugt einen User-Outcall zur angebenen Rufnummer (kanonisches Format) - SMS-Rufnummer siehe Eigene persönliche Daten, Inhalt der SMS siehe Templates
Profile	Profil für persönlichen AutoAttendant
Profile: Besetzt, Nicht angenommen, Besprechung, Krank, Pause, Außer Haus, Urlaub, Mittagspause, Zu Hause	Ein Anrufer kann durch Nachwahl einer Ziffer von 0 bis 9 auf ein Weiterleitungsziel geführt werden oder eine Nachricht aufsprechen. Voraussetzung ist eine Ansage je Anwesenheitsstatus.
Profile: Dynamische Ansage überspringen	Die automatische Ansage des Anwesenheitsstatus wird überprungen, statt dessen hört ein Anrufer nur die Ansage des Namens und dann des persönlichen AutoAttendant
Sensibilität	Einstellungen zur Wahrung der Vertraulichkeit
Sensibilität: Sicherheit und Zugriff	Freigabe der Sprachnachrichten für myAttendant; Abfrage der Sprachbox vom eigenen Telefon ohne Kennwort
Sensibilität: Sichtbarkeit des Anwesenheitsstatus	Festlegung der Sichtbarkeit des eigenen Anwesenheitsstatus für die internen Benutzer
Sensibilität: VoiceMail-Anwesenheitsstatus	Ansage Ihres Anwesenheitsstatus für externe Anrufer. Eingabe von zu sperrenden internen Telefonnummern, es können Wildcards verwendet werden.
myAttendant	Anzeige nur bei Teilnehmern, die für myAttendant lizenziert sind
myAttendant: LAN-Nachrichten	Textbausteine für Sofortnachrichten von myAttendant, freie Eingabe, Auswahl im Chat Fenster des Clients
myAttendant: DuWas	Eingabe von Durchwahlnummern; falls myAttendant für mehrere Firmen verwendet werden soll, kann ein "Für"-Fenster eingeblendet werden
myAttendant: Kommunikation	Eingabe einer internen Nummer für Anrufweiterleitungen im Notfall oder bei Nichtannahme durch myAttendant (für USA)

27.4.3.3 OpenScape Business UC Suite > Abteilungen

Parameterbeschreibung der Registerkarten:

- **Abteilungen**

Parameter	Beschreibung
Name der Abteilung	Abteilungen gruppieren Teilnehmer im internen Verzeichnis nach ihrer organisatorischen Zugehörigkeit. Damit kann z. B. in myAttendant eine automatische Zuordnung der Benutzer zu den Abteilungen erfolgen.
Gruppennummer	(interne Nummerierung ohne weitere Bedeutung)

27.4.3.4 OpenScape Business UC Suite > Gruppen

Durch eine Voicemail-Gruppe (Sprachbox-Gruppe) kann einer Teilnehmergruppe der Zugriff auf Sprachnachrichten ermöglicht werden. Über die Rufnummer der Voicemail-Gruppe werden nicht die Mitglieder dieser Gruppe gerufen, sondern wird direkt die Voicemail (die Sprachbox) der Gruppe erreicht.

Durch eine Fax-Gruppe (Faxbox-Gruppe) kann einer Teilnehmergruppe der Zugriff auf Faxnachrichten ermöglicht werden. Über die Rufnummer der Fax-Gruppe wird direkt die Faxbox der Gruppe erreicht.

Parameterbeschreibung der Registerkarten:

- **Voicemail-Gruppen**
- **Fax-Gruppen**

Parameter	Beschreibung
Voicemail-Gruppen	
Voicemail-Gruppe	Name der Voicemail-Gruppe
Pilot	Rufnummer der Voicemail-Gruppe
Typ	Typ der Voicemail-Gruppe
Anzahl Benutzer	Anzahl der Mitglieder der Voicemail-Gruppe
Anzahl Nachrichten	Anzahl der neuen Sprachnachrichten für die Voicemail-Gruppe
Benutzer	Mitglieder der Voicemail-Gruppe
Fax-Gruppen	
Fax-Gruppe	Name der Fax-Gruppe
Pilot	Rufnummer der Fax-Gruppe
Anzahl Benutzer	Anzahl der Mitglieder der Fax-Gruppe
Anzahl Faxnachrichten	Anzahl der neuen Faxnachrichten für die Fax-Gruppe
Benutzer	Mitglieder der Fax-Gruppe

27.4.3.5 OpenScape Business UC Suite > Templates

Parameterbeschreibung der Registerkarten:

- **SMS-Templates**

Parameter	Beschreibung
Bearbeiten	Im Feld Empfänger, Betreff oder Text können Platzhalter eingefügt werden, die man jeweils unter "VSL-Felder" auswählt.

27.4.3.6 OpenScape Business UC Suite > Externes Verzeichnis

Parameterbeschreibung der Registerkarten:

- **Externes Verzeichnis**

Parameter	Beschreibung
	Manuelles Hinzufügen einzelner Kontakte zum externen Verzeichnis. Die Zeichen müssen dem UTF-8 Format entsprechen (z. B. werden keine Umlaute dargestellt)

Parameterbeschreibung der Registerkarten:

- **Externes Verzeichnis importieren**

Parameter	Beschreibung
XMPP-ID	Adresse eines externen Benutzers der über XMPP in UC Suite eingebunden wird, für Instant Messaging und die Übermittlung von Anwesenheitsstatus (Format mueller@unify.com/home)

27.4.3.7 OpenScape Business UC Suite > Externer Anbieter

Parameterbeschreibung der Registerkarten:

- **Kontaktanbieter > Exchange**

Parameter	Beschreibung
Hinzufügen/Bearbeiten	Eingabe der Zugangsdaten des Exchange-Servers. In einer Microsoft-Umgebung ist der Active Directory Server (ADS) bzw. der Exchange Server auch gleichzeitig der LDAP-Server.
Name	Name dieses Externen Offline-Verzeichnisses.
Serveradresse	DNS-Name oder IP-Adresse des Exchange-Servers.
Benutzername / Kennwort	Benutzername und Kennwort für den Zugriff auf den externen Exchange-Server.

Parameterbeschreibung der Registerkarten:

- **Kontaktanbieter > LDAP**

Parameter	Beschreibung
Hinzufügen/Bearbeiten	Zugangsdaten des LDAP-Servers.
Name	Name für dieses Externe Offline-Verzeichnis
Serveradresse	DNS-Name oder IP-Adresse des LDAP-Servers.
Port	Portnummer des externen LDAP-Servers

Parameter	Beschreibung
Benutzername / Kennwort	Benutzername und Kennwort für den Zugriff auf den externen LDAP-Server.
LDAP Basis-DN	LDAP Base Distinguished Name ein, z. B. dc=example-for-a-domain, dc=net.
Anrede, **Vorname**, **Nachname**, **Geschäftlich 1**, **Geschäftlich 2**, **Privat**, **Mobil**, **Firma**, **Firmen-Rufnr.**, **Postanschrift**, **Bundesland oder Region**, **Land**, **Postleitzahl**, **E-Mail**, **Pager**, **Fax-rufnummer**, **XMPP-ID** und **Stadt**	Bei der Konfiguration eines Externen Offline-Verzeichnisses kann der Administrator das Mapping der Felder an die Namen des verwendeten LDAPServers anpassen. Gelöschte Felder werden bei der Suche nach Namen mittels Rufnummer ignoriert. Die Suche erfolgt immer mit den letzten 4 Stellen der Rufnummer mit vorangestellter Wildcard. Sie können die Suche nach Namen mittels Rufnummer bei kommenden Gesprächen deaktivieren. Geben Sie jeweils die entsprechende Feldbezeichnung des LDAP-Servers ein.

Parameterbeschreibung der Registerkarten:

- **Kontaktanbieter > MSSQL**

Parameter	Beschreibung
Hinzufügen/Bearbeiten	Zugangsdaten des Microsoft SQL Servers
Name	Name für dieses Externe Offline-Verzeichnis
Serveradresse	DNS-Namen oder IP-Adresse des Microsoft SQL-Servers
Benutzername / Kennwort	Benutzername und Kennwort für den Zugriff auf den Microsoft SQL-Server
DB-Name	Name der Datenbank.

Parameterbeschreibung der Registerkarten:

- **Kalenderanbieter > Exchange**

Parameter	Beschreibung
Exchange-Kalender integrieren	Die Kalenderintegration dient zur automatischen Erstellung von Outlook-Terminen bei Abwesenheit unter Windows. Wenn die Outlook-Termine nicht in der lokalen PST-Datei des Benutzers, sondern auf dem Exchange-Server gespeichert werden sollen, müssen hier die Zugriffsdaten eingegeben werden.
Exchange-Kalender-Integration aktivieren	Aktivieren der Exchange-Kalenderintegration
Server URL	Details zur Nutzung der verschiedenen Microsoft Exchange Server Versionen finden Sie im Unify Experts Wiki unter `http://wiki.unify.com/wiki/OpenScape_Business#Microsoft_Exchange_Server`.

27.4.3.8 OpenScape Business UC Suite > Contact Center

Parameterbeschreibung der Registerkarten:

- **Zeitplan**
- **Warteschlange**
- **Servicegrad**
- **VIP-Anruferprioritäten**
- **VIP-Rufliste**
- **Bevorzugte Agenten**

- **Contact Center Pausen**
- **Einfache Nachbearbeitung**
- **Mehrfache Nachbearbeitung**
- **Warteschlangen-Bindungen**

Zeitplan

Über einen Zeitplan wird definiert, wie kommende Anrufe an bestimmten Tagen und zu bestimmten Zeiten behandelt werden sollen. Für jede Warteschlange wird über einen Zeitplan und die darin enthaltenen Regeln (Call Control Vector CCV) definiert, wie kommende Anrufe an bestimmten Tagen und zu bestimmten Zeiten behandelt werden sollen. Einem Zeitplan muss mindestens eine Regel (Call Control Vector CCV) zugeordnet werden. Die Regeln bestimmen für den Zeitraum für den ein Zeitplan gilt, wie kommende Anrufe in einer Warteschlange behandelt werden. Regeln gelten ausschließlich für Anrufe und nicht für Faxe und E-Mails.

Ausführliche Informationen zur Konfiguration von Zeitplänen siehe Vorgehensweise bei der Konfiguration

Parameter	Beschreibung
Zeitplan	Name des Zeitplans
Warteschlange	Name der Warteschlange, der der Zeitplan zugeordnet ist.
Gruppennummer	Rufnummer der UCD-Gruppe, die bei der Grundkonfiguration des Contact Centers eingerichtet wurde.
Zeitplan	
Name des Zeitplans	Name des Zeitplans
Standard-CCV	Angezeigt wird die Standard-Regel für diesen Zeitplan, die nach Zuweisung zu einer Warteschlange 24 Stunden am Tag und 365 Tage im Jahr gilt. Sollen zu bestimmten Zeiten (Pause, Wochenende, Feiertag, Urlaub usw.) andere Regeln gelten, können diese dem entsprechenden Zeitplan als Ausnahme-Regeln (Ausnahme-CCV) zugeordnet werden.
Warteschlangen	
Name der Warteschlange	Name der Warteschlange, der dieser Zeitplan zugeordnet ist.
Warteschlange aktiv	Zeigt an, ob die Warteschlange aktiv oder inaktiv ist.
Ausnahmen	
CCV	Name der Ausnahme-Regel (Ausnahme-CCV) Ausnahme-Regeln definieren, wie kommende Anrufe zu bestimmten Ausnahmezeiten (Pause, Wochenende, Feiertag, Urlaub usw.) behandelt werden. Urlaubspläne haben hierbei Vorrang vor anderen Zeitplänen und Regeln einer Warteschlange.
Beschreibung	Beschreibender Text für die Ausnahme-Regel
Typ	Typ der Ausnahme-Regel
Startdatum	Datum für den Beginn der Ausnahme-Regel

Parameter	Beschreibung
Endedatum	Datum für das Ende der Ausnahme-Regel
Startzeit	Uhrzeit für den Beginn der Ausnahme-Regel
Endezeit	Uhrzeit für das Ende der Ausnahme-Regel

Warteschlange

Warteschlangen sind die Basis des Contact Centers. Anrufe, Faxe und E-Mails für eine Warteschlange können in Abhängigkeit vom Fähigkeits-Level der Agenten, von der Priorität und der Wartezeit behandelt werden. Anrufern, die sich im Wartezustand befinden, können Ansagen eingespielt werden.

Ausführliche Informationen zur Konfiguration von Warteschlangen siehe Vorgehensweise bei der Konfiguration

Parameter	Beschreibung
Warteschlange	Name der Warteschlange
Warteschlange aktiv	Zeigt an, ob die Warteschlange aktiv oder inaktiv ist.
Pilot	Rufnummer (Pilot) für eingehende Faxnachrichten Faxe an diese Rufnummer werden in die Warteschlange übernommen und wie kommende Anrufe behandelt.
Allgemeine Einstellungen	
Name der Warteschlange	Name der Warteschlange
Warteschlange aktiv	Definition des Warteschlangenzustands
Warteschlange aktiv: Nicht Aktiv	Die Warteschlange ist nicht aktiv.
Warteschlange aktiv: Aktiv	Die Warteschlange ist aktiv.
Gruppennummer	Rufnummer der UCD-Gruppe ein, die bei der Grundkonfiguration des Contact Centers eingerichtet wurde.
Telefonanlage	Angezeigt wird der Eintrag CSP
Zeitplan	Angezeigt wird der zugeordnete Zeitplan
Anzahl Warteschlangen-Alarme	Alarm-Schwellwertanzahl Wird die hier angegebene Anzahl wartender Anrufe in der Warteschlange überschritten, wechselt das Warteschlangensymbol bei den Agenten von grün auf orange. Standardwert: 3 Anrufe
Zeit Warteschlangen-Alarm	Alarm-Schwellwertzeit in Sekunden Wird die hier angegebene Wartezeit eines Anrufs in der Warteschlange überschritten, wechselt der betreffende Eintrag in der Liste der Contact-Center-Anrufe bei den Agenten auf rot. Standardwert: 5 Sekunden

Parameter	Beschreibung
Zeitüberschreitung für entgangene Anrufe	Zeitüberschreitung für entgangene Anrufe in Sekunden Nach Ablauf der hier angegebenen Zeit wird ein nicht angenommener Anruf zum nächsten freien Agenten weitergeleitet. Standardwert: 5 Sekunden
Schwellwert für abgebrochene Anrufe	Schwellwertzeit für abgebrochene Anrufe in Sekunden Die hier angegebene Zeit legt fest, ob ein abgebrochener Anruf in die Statistik (in einen Bericht) aufgenommen wird oder nicht. Statistisch erfasst werden Anrufe, die nach Ablauf der angegebenen Zeit abgebrochen werden. Standardwert: 5 Sekunden
Popup-Fenster aktiviert	Bei aktiviertem Flag erscheint in myAgent bei kommenden Anrufen ein PopUp-Fenster zur Anzeige und Eingabe von Kundendaten. PopUp-Fenster sind erforderlich, um Rückrufe anzunehmen und auszuführen und um Faxe und E-Mails anzunehmen. Standardwert: Deaktiviert
Nachbearbeitungsmodus	Definition des Nachbearbeitungsmodus
Nachbearbeitungsmodus: Keine Nachbearbeitung	Für die Warteschlange können keine Nachbearbeitungsgründe definiert werden.
Nachbearbeitungsmodus: Einfache Nachbearbeitung	Für die Warteschlange können ein oder mehrere Nachbearbeitungsgründe definiert werden.
Nachbearbeitungsmodus: Mehrfache Nachbearbeitung	Für die Warteschlange können ein oder mehrere Nachbearbeitungsgründe definiert und in Gruppen und Untergruppen zusammengefasst werden.
Prioritäten	Ist ein Agent mehreren Warteschlangen zugeordnet, kann festgelegt werden, ob die Anrufe für eine Warteschlange mit höherer Priorität an diesen Agenten weitergeleitet werden sollen als die Anrufe für andere Warteschlangen.
Warteschlangen-Pilots	
Pilots für eingehende Faxnachrichten	Rufnummern (Pilots) für eingehende Faxnachrichten Faxe an diese Rufnummern werden in die Warteschlange übernommen und wie kommende Anrufe behandelt.
Dienst für eingehende E-Mails	E-Mail-Adressen für eingehende E-Mails E-Mails an diese Adressen werden in die Warteschlange übernommen und wie kommende Anrufe behandelt.
Verschiedenes	
Absender-E-Mail-Adresse	Absender-E-Mail-Adresse für verschickte E-Mails Die hier angegebene E-Mail-Adresse wird beim Versenden einer E-Mail durch einen Agenten beim Empfänger angezeigt.
Intelligente Anrufweiterleitung	Bei aktiviertem Flag werden kommende Anrufe automatisch an den Agenten weitergeleitet, der zuletzt mit dem Anrufer verbunden war. Voraussetzung ist, dass für den Anrufer keine bevorzugten Agenten festgelegt wurden. Standardwert: Deaktiviert

Servicegrad

Anhand des Servicegrads können Aussagen über die Beantwortungsqualität einer Warteschlange getroffen werden. Ermöglicht wird dies durch den Vergleich der Anruferwartezeiten in einer Warteschlange mit Sollwerten, die hier für jede Warteschlange individuell vorgegeben werden können.

Für jeden Anruf an eine entsprechende Warteschlange wird der Servicegrad nach Beendigung des Anrufs ermittelt und in die Datenbank übernommen. Eine Auswertung des Servicegrads können Agenten mit dem Berechtigungs-Level Supervisor oder Administrator über die Applikation myAgent vornehmen.

Ausführliche Informationen zur Definition von Sollwerten für den Servicegrad siehe Vorgehensweise bei der Konfiguration

Parameter	Beschreibung
Warteschlange	Name der Warteschlange
Warteschlange aktiv	Zeigt an, ob die Warteschlange aktiv oder inaktiv ist.
Gruppennummer	Rufnummer der UCD-Gruppe ein, die bei der Grundkonfiguration des Contact Centers eingerichtet wurde.
Servicegrad	Die horizontale Achse zeigt die Wartezeit in der Warteschlange in Intervallen von 10 Sekunden, die vertikale Achse den Sollwert für den Servicegrad in Prozentwerten. Die roten Punkte geben die Sollwerte für die Vermittlungsqualität der Warteschlange vor. Durch den Vergleich der Sollwerte mit den tatsächlichen Anruferwartezeiten können Qualitätsaussagen getroffen werden.

VIP-Anruferprioritäten

Anhand der VIP-Anruferpriorität kann für jede Warteschlange individuell definiert werden, ob die in der VIP-Rufliste enthaltenen Anrufer bevorzugt behandelt werden sollen.

Die Werte für die VIP-Anruferpriorität können in Abhängigkeit von der Anruferwartezeit in einer Warteschlange frei bestimmt werden. Damit wird der Grad der Bevorzugung von VIP-Anrufern gegenüber normalen Anrufern festgelegt.

Aktiviert ein VIP-Anrufer einen Agentenrückruf (Aufnahme einer Sprachnachricht mit Rückrufwunsch) verbleibt der Agentenrückruf anstelle des VIP-Anrufers in der Warteschlange. Die VIP-Anruferpriorität wird dabei nicht übernommen.

Ausführliche Informationen zur Definition der VIP-Anruferpriorität siehe Vorgehensweise bei der Konfiguration

Parameter	Beschreibung
Warteschlange	Name der Warteschlange
Warteschlange aktiv	Zeigt an, ob die Warteschlange aktiv oder inaktiv ist.
Gruppennummer	Rufnummer der UCD-Gruppe ein, die bei der Grundkonfiguration des Contact Centers eingerichtet wurde.
VIP-Anruferpriorität	Die horizontale Achse zeigt die Wartezeit in der Warteschlange in Intervallen von 30 Sekunden, die vertikale Achse die Priorität normaler Anrufer, die nicht in der VIP-Rufliste verzeichnet sind. Die roten Punkte definieren die Priorität normaler Anrufer gegenüber VIP-Anrufern.

VIP-Rufliste

Bereits im Kommunikationssystem erfasste Anrufer (externes Verzeichnis) können in die VIP-Rufliste übernommen werden. Darüber hinaus ist die Eingabe von Rufnummernmustern möglich. Rufnummernmuster setzen sich aus einer bestimmten Ziffernfolge und einer Wildcard (Platzhalter) zusammen. Damit können beispielsweise alle Mitarbeiter eines Unternehmens in die VIP-Rufliste übernommen werden.

Ausführliche Informationen zur Konfiguration der VIP-Rufliste siehe Vorgehensweise bei der Konfiguration

Parameter	Beschreibung
Warteschlange	Name der Warteschlange
Warteschlange aktiv	Zeigt an, ob die Warteschlange aktiv oder inaktiv ist.
Gruppennummer	Rufnummer der UCD-Gruppe ein, die bei der Grundkonfiguration des Contact Centers eingerichtet wurde.
VIP-Rufliste	Angezeigt werden die in der VIP-Rufliste enthaltenen Anrufer und Rufnummernmuster. Je weiter rechts sich der Scrollbalken bei einem Anrufer oder Rufnummernmuster befindet, desto höher ist die Priorität gegenüber den anderen in der VIP-Rufliste enthaltenen Anrufern oder Rufnummernmustern.

Bevorzugte Agenten

Jedem Anrufer können ein oder mehrere bevorzugte Agenten einer Warteschlange zugeordnet werden. In diesem Fall versucht das Kommunikationssystem, den Anrufer und die Rückrufwünsche dieses Anrufers zunächst an einen bevorzugten Agenten zu vermitteln. Wurden mehrere bevorzugte Agenten festgelegt, kann eine Priorität (Reihenfolge) definiert werden, mit der die bevorzugten Agenten vermittelt werden.

Ist kein bevorzugter Agent verfügbar, wird der Anruf an einen beliebigen verfügbaren Agenten weitergeleitet.

Ausführliche Informationen zur Definition bevorzugter Agenten siehe Vorgehensweise bei der Konfiguration

Parameter	Beschreibung
Warteschlange	Name der Warteschlange
Warteschlange aktiv	Zeigt an, ob die Warteschlange aktiv oder inaktiv ist.
Gruppennummer	Rufnummer der UCD-Gruppe ein, die bei der Grundkonfiguration des Contact Centers eingerichtet wurde.
Bevorzugte Agenten	Angezeigt werden die bevorzugten Agenten der in der Kundenliste genannten Anrufer Wurden für einen Anrufer mehrere bevorzugte Agenten definiert, zeigt die Listenposition die Priorität gegenüber den anderen bevorzugten Agenten. Je höher ein Agent in der Liste positioniert ist, desto höher ist seine Priorität.
Nur Kunden mit Zuweisung zu Agenten anzeigen	Bei aktiviertem Flag werden in der Kundenliste nur Anrufer angezeigt, für die mindestens ein bevorzugter Agent festgelegt wurde. Standardwert: Deaktiviert

Contact Center Pausen

Um jedem Agenten definierte Pausen zu ermöglichen, können unterschiedlich lange Contact Center-Pausen festgelegt werden. Contact Center-Pausen stehen systemweit zur Verfügung und können bei Bedarf von einem Agenten über myAgent ausgewählt werden.

Ausführliche Informationen zur Definition von Contact Center-Pausen siehe Vorgehensweise bei der Konfiguration

Parameter	Beschreibung
Name	Name der Contact Center-Pause
Dauer	Dauer der Contact Center-Pause in Minuten
Aktiv	Zeigt an, ob die Contact Center-Pause aktiv oder inaktiv ist.

Einfache Nachbearbeitung

Für Warteschlangen mit dem Nachbearbeitungsmodus "Einfache Nachbearbeitung" können hier ein oder mehrere Nachbearbeitungsgründe definiert werden.

Anhand von Nachbearbeitungsgründen können kommende Anrufe bestimmten Themen (Bestellung, Reklamation, Service usw.) zugeordnet werden. Die Zuordnung trifft ein Agent nach Gesprächsende (in der Nachbearbeitungszeit) über myAgent, durch Auswahl des betreffenden Nachbearbeitungsgrunds.

Ausführliche Informationen zur Definition von Nachbearbeitungsgründen (Nachbearbeitungscodes) siehe Vorgehensweise bei der Konfiguration

Parameter	Beschreibung
Warteschlange	Name der Warteschlange, für die Einfache Nachbearbeitung konfiguriert wurde.
Beschreibung	Beschreibender Text für den Nachbearbeitungsgrund

Mehrfache Nachbearbeitung

Für Warteschlangen mit dem Nachbearbeitungsmodus "Mehrfache Nachbearbeitung" können hier ein oder mehrere Nachbearbeitungsgründe definiert und in Gruppen und Untergruppen zusammengefasst werden.

Anhand von Nachbearbeitungsgründen können kommende Anrufe bestimmten Themen (Bestellung, Reklamation, Service usw.) zugeordnet werden. Die Zuordnung trifft ein Agent nach Gesprächsende (in der Nachbearbeitungszeit) über myAgent, durch Auswahl des betreffenden Nachbearbeitungsgrunds.

Ausführliche Informationen zur Definition von Nachbearbeitungsgründen (Nachbearbeitungscodes) siehe Vorgehensweise bei der Konfiguration

Parameter	Beschreibung
Warteschlange	Name der Warteschlange, für die Mehrfache Nachbearbeitung konfiguriert wurde. Angezeigt werden die für diese Warteschlange bereits definierten Gruppen und Untergruppen.
Beschreibung	Beschreibender Text für den Nachbearbeitungsgrund

Warteschlangen-Bindungen

Über die Warteschlangen-Bindungen können Agenten einer oder mehreren Warteschlangen zuordnet werden.

Ausführliche Informationen zur Zuordnung von Agenten zu Warteschlangen siehe Vorgehensweise bei der Konfiguration

Parameter	Beschreibung
Warteschlange	Name der Warteschlange
Warteschlange aktiv	Zeigt an, ob die Warteschlange aktiv oder inaktiv ist.
Gruppennummer	Rufnummer der UCD-Gruppe ein, die bei der Grundkonfiguration des Contact Centers eingerichtet wurde.
Agent	Agent, der der Warteschlange zugeordnet ist.
Agentenzuweisung	
Typ	Agententyp Möglich sind folgende Optionen: • Hauptagent: Der Agent erhält Anrufe unabhängig von der Auslastung der Warteschlange. • Agent bei Überlauf: Der Agent erhält Anrufe nur bei Überlauf der Warteschlange.
Überlauf nach Sekunden in Warteschlange	Nur für Agent bei Überlauf: Überlaufzeit in Sekunden Nach Ablauf der Überlaufzeit wird ein Anruf an einen Agenten bei Überlauf weitergeleitet.
Überlauf nach Anrufen in Warteschlange	Nur für Agent bei Überlauf: Anzahl der Anrufe Anrufe, die über diese Maximalzahl hinausgehen, werden an einen Agenten bei Überlauf weitergeleitet.
Fähigkeits-Level	Anzeige des Fähigkeits-Levels in Prozent Das Fähigkeits-Level steuert die Verteilung der Anrufe auf die Agenten in einer Warteschlange. Agenten mit höherem Fähigkeits-Level werden bei der Anrufverteilung bevorzugt. Haben alle Agenten das gleiche Fähigkeits-Level, erhält der am längsten freie Agent den Anruf.
Agentenrückruf aktivieren	Bei aktiviertem Flag erhält der Agent Rückrufwünsche in Form von Sprachnachrichten.
Nachbearbeitung	Automatische Nachbearbeitungszeit in Sekunden

27.4.3.9 OpenScape Business UC Suite > Zeitpläne

Parameterbeschreibung der Registerkarten:

- **Bearbeiten/Hinzufügen**

Parameter	Beschreibung
Auto-Vermittlungsplatz	Konfiguration der AutoAttendant-Funktion der UC Suite (Company AutoAttendant)
Zeitplan bearbeiten	Über einen Zeitplan und die darin enthaltenen Regeln (Call Control Vector CCV) wird definiert, wie kommende Anrufe an bestimmten Tagen und zu bestimmten Zeiten behandelt werden sollen.
Name des Zeitplans	Der Zeitplan kann unter einem frei definierbaren Namen gespeichert werden. Es wird empfohlen, hier einen sinnvollen Namen einzugeben.
Standard-CCV	Dem Zeitplan muss mindestens eine Regel (Call Control Vector CCV) zugeordnet werden. Regeln bestimmen für den betreffenden Zeitraum, wie kommende Anrufe behandelt werden. Regeln gelten ausschließlich für Anrufe und nicht für Faxe und E-Mails. Regeln werden mit dem graphischen Regel-Editor (CCV-Editor) durch die Verknüpfung von vordefinierten CCV-Objekten erstellt. Es sind mehrere vorbelegte, standardisierte Vorlagen verfügbar, die beliebig verändert und an den speziellen Bedarf angepasst werden können.
Bearbeiten/Hinzufügen	Bearbeiten der ausgewählten Regel oder Hinzufügen einer neuen (öffnet den Regel-Editor)
Warteschlangen	Es wird empfohlen, nur eine Warteschlange je Zeitplan zu aktivieren (nur ein Häkchen setzen).
Name der Warteschlange	Die Warteschlange kann unter einem frei definierbaren Namen gespeichert werden. Es wird empfohlen, hier einen sinnvollen Namen einzugeben.
Warteschlange aktiv	Die Warteschlange kann aktiviert oder deaktiviert werden.
Zeitplan	Auswahl des zugehöriger Zeitplans
Pilot	Rufnummer des zugehörigen virtuellen Ports im Kommunikationssystem.
Ausnahmen	Ein Zeitplan mit einer Standard-Regel gilt nach Zuweisung zu einer Warteschlange 24 Stunden am Tag und 365 Tage im Jahr. Sollen zu bestimmten Zeiten (Pause, Wochenende, Feiertag, Urlaub usw.) andere Regeln gelten, können diese dem entsprechenden Zeitplan als Ausnahme-Regeln (Ausnahme-CCV) zugeordnet werden. Damit kann definiert werden, wie kommende Anrufe beispielsweise während der Urlaubszeit behandelt werden sollen. Urlaubspläne haben hierbei Vorrang vor anderen Zeitplänen und Regeln.
CCV	Auswahl der Ausnahme-Regel (Ausnahme-CCV)
Beschreibung	Freie Eingabe einer Beschreibung für den Ausnahme-Zeitplan
Typ	Im Zeitbereich innerhalb eines oder mehrerer Wochentage / Im Zeit-/Datumsbereich frei definierbar / Urlaubspläne für einen Datumsbereich
Startdatum	Beginn der Ausnahme (Datum)
Endedatum	Ende der Ausnahme (Datum)
Startzeit	Beginn der Ausnahme (Uhrzeit)
Endezeit	Ende der Ausnahme (Uhrzeit)
(Wochentag)	Die Ausnahme soll an einem oder mehreren Wochentagen gelten

27.4.3.10 OpenScape Business UC Suite > Datei-Upload

Parameterbeschreibung der Registerkarten:

- **Upload von Audiodateien**

Parameter	Beschreibung
Upload-Ziel	Applikation, für welche die neue Ansage verwendet wird
Upload-Ziel: Auto-Vermittlungs-platz	Ansagen für die automatische Vermittlung
Upload-Ziel: Profile	Ansagen für alle oder einzelne Benutzer von UC Suite
Upload-Ziel: Voicemai-Begrü-ßung	Sprachbox-Begrüßungen für alle oder einzelne Benutzer von UC Suite
Upload-Ziel: VM-Gruppenbegrü-ßung	Begrüßung für eine Gruppen-Sprachbox
no key for: uploader	Die Ansage liegt zum Upload als PCM-Dateie vor, mit folgenden Eigenschaften: 8 kHz, 16 bit, mono. Die Länge des Audio-Dateinamens beträgt maximal 30 Zeichen.
Aufzeichnungsgerät	Die Ansage wird über das Telefon einer Nebenstelle aufgenommen
Audiodatei	
Download	Heruntergeladene Ansagen.
Löschen	Heruntergeladene Ansagen löschen.
Umbenennen	Heruntergeladene Ansagen umbenennen.
Aufzeichnungsgerät	
Dateiname	Angabe des Dateinamens der aufzuzeichnenden Ansage.
Nebenstelle	Auswahl des Telefons, mit dem die Ansage aufgezeichnet werden soll.
Anrufen	Ruft das Telefon an, mit dem die Ansage aufgezeichnet werden soll.
Wiedergeben	Gibt die aufgenommene Ansage wieder.
Aufzeichnen	Startet die Aufzeichnung der Ansage.

Parameterbeschreibung der Registerkarten:

- **Upload des zentralen Fax-Deckblatts**

Parameter	Beschreibung
Upload des zentralen Fax-Deckblatts	
Ocp Datei	Fax-Deckblatt liegt als .ocp Datei
Name	
Beschreibung	

27.4.3.11 OpenScape Business UC Suite > Konferenzschaltung

Parameterbeschreibung der Registerkarten:

- **Konferenzschaltung**

Parameter	Beschreibung
Name	Name der Konferenz (vom Benutzer vergeben)
Besitzer	Name des Benutzers, der die Konferenz initiiert hat
Als nächste geplant	Nächste geplante Startzeit
Aktiv	
Anzahl Mitglieder	Anzahl der Konferenzmitglieder einschließlich Konferenzleiter
Anzeige	Teilnehmer der ausgewählten Konferenz

27.4.3.12 OpenScape Business UC Suite > Standort-Liste

Parameterbeschreibung der Registerkarten:

- **Standort-Liste**

Parameter	Beschreibung
Standort-Name	Standorte im vernetzten Kommunikationssystem (siehe Grundeinstellungen > Gateway-Eigenschaften)
Standort-Adresse	IP-Adresse von UC Booster Card, von UC Booster Server oder des Kommunikations-systems
Standort-Port	Server Port
Standort-IP-Trunks	Standort-IP-Trunks, sofern vorhanden
Online-Status	Verbindungsstatus des Kommunikationssystems am Standort

27.4.3.13 OpenScape Business UC Suite > Server

Parameterbeschreibung der Registerkarten:

- **Allgemeine Einstellungen**
- **Gespräch aufzeichnen**
- **Protokolle**
- **Benachrichtigungen**
- **Wartung**
- **Sprachnachrichten**

Parameter	Beschreibung
Bürozeiten	
Startzeit	Beginn der täglichen Bürozeit (Geschäftszeit) Einstellung für den Anwesenheitsstatus der UC Clients Standardwert: 7:00 Uhr
Endezeit	Ende der täglichen Bürozeit (Geschäftszeit) Einstellung für den Anwesenheitsstatus der UC Clients Standardwert: 19:00 Uhr
Kennwortlänge	
Längen	Länge der Kennworts für die UC Clients ***HINWEIS:*** Durch das Ändern der Kennwortlänge werden die Kennwörter aller Benutzer zurückgesetzt. Standardwert: 6
Rufnummer des Abwurfplatzes	
Zielnummer	Rufnummer des Abwurfplatzes ***INFO:*** Einzutragen ist die im Kommunikationssystem konfigurierte Rufnummer des Abwurfplatzes.
Sofortnachricht	
Sofortnachricht versenden deaktivieren	Bei aktiviertem Flag ist kein Versand von Sofortnachrichten möglich. Standardwert: Deaktiviert
Analoge Nebenstellen	
Modus Analoger Teilnehmer	Definition der Anzeige analoger Teilnehmer im internen Verzeichnis Standardwert: Alle anzeigen
Modus Analoger Teilnehmer: Alle anzeigen	Alle analogen Teilnehmer werden im internen Verzeichnis angezeigt
Modus Analoger Teilnehmer: Nur Benannte anzeigen	Ausschließlich analoge Teilnehmer mit einem Namen werden im internen Verzeichnis angezeigt.
Modus Analoger Teilnehmer: Nicht anzeigen	Kein analoger Teilnehmer wird im internen Verzeichnis angezeigt.
Nebenstelle	
Max. interne Länge	Maximale Ziffernanzahl bei internen Rufnummern Zum Schutz vor Gebührenmissbrauch ist die Wahl längerer interner Rufnummern nicht möglich. Standardwert: 4
Min. externe Länge	Minimale Ziffernanzahl bei externen Rufnummern Standardwert: 3
Übergabe	

Parameter	Beschreibung
Normales Vermittlungsplatz-SST	Bei aktiviertem Flag erfolgt die Übergabe eines Anrufs, unabhängig davon, ob das Ziel frei, besetzt oder nicht verfügbar ist. Standardwert: Aktiviert
Gespräch aufzeichnen	
Gespräch aufzeichnen	Bei aktiviertem Flag ist das Aufzeichnen von Anrufen und Konferenzen möglich. Standardwert: Aktiviert
Vor der Aufzeichnung eine Ansage wiedergeben	Bei aktiviertem Flag wird vor dem Beginn einer Aufzeichnung eine Ansage wiedergeben. Standardwert: Deaktiviert
Während der Aufzeichnung einen Hinweiston wiedergeben	Bei aktiviertem Flag wird während der Aufzeichnung ein Hinweiston eingespielt. Standardwert: Aktiviert
Systemprotokolle	
Trace-Meldungen protokollieren (ausführlich)	Bei aktiviertem Flag werden Trace-Meldungen täglich in einer Protokolldatei aufgezeichnet. Standardwert: Deaktiviert
Client-Logs	
Client-Log-Pfad	Ablagepfad für Client-Log-Dateien (Protokolldateien der UC Suite)
Protokoll-Upload aktivieren	Bei aktiviertem Flag werden Client-Logs auf der Festplatte der UC Booster Card (OCAB), des UC Booster Servers oder des Kommunikationssystems OpenScape Business S abgelegt. Standardwert: Aktiviert
Client-Protokollierung aktivieren	Bei aktiviertem Flag werden Client-Logs aufgezeichnet. Standardwert: Aktiviert
E-Mail-Benachrichtigungen	
E-Mail-Benachrichtigungen bei Systemfehlern aktivieren	Bei aktiviertem Flag werden E-Mails verschickt, um den oder die eingetragenen Empfänger zum Beispiel vor einem kritischem Füllstand der Festplatte zu warnen oder über Fehler zu informieren. Standardwert: Aktiviert
myPortal Einladungs-E-Mail deaktivieren	Bei aktiviertem Flag werden Konferenzteilnehmer nicht automatisch per E-Mail über Konferenzen informiert. Standardwert: Deaktiviert
Empfänger	E-Mail-Adressen, an die E-Mail-Benachrichtigungen verschickt werden.
Bedingungen	
Wichtige Benachrichtigungen senden	Bei aktiviertem Flag erfolgt eine E-Mail-Benachrichtigung bei wichtigen Benachrichtigungen, wie zum Beispiel bei Systemfehlern Standardwert: Aktiviert
Benachrichtigungen über Systemabsturz senden	Bei aktiviertem Flag erfolgt eine E-Mail-Benachrichtigung bei Systemabstürzen. Standardwert: Aktiviert

Parameter	Beschreibung
Bei Fehlermeldungen die letzten … Zeilen der Protokolldatei senden	Definition der Anzahl der Zeilen einer Protokolldatei, die mit einer E-Mail verschickt werden sollen. Standardwert: 100
Wartung	
Systemwartung beginnen um	Definition der Uhrzeit, zu der täglich das Löschen folgender Daten erfolgt, die die jeweils eingestellten Aufbewahrungszeiten überschritten haben: • Nachrichten • Anrufinformationen im Anrufjournal (Anrufhistorie) • Mit myAgent aufgezeichnete Anrufe (Contact Center) • Empfangene und gesendete Faxe und E-Mails für das Contact Center • Protokolldateien Standardwert: 2:00 Uhr
Nachricht	
Nachrichten im Posteingang aufbewahren für	Aufbewahrungsdauer in Tagen für Sprachnachrichten im Posteingang Standardwert: 60
Abgespielte / gelesene Nachrichten aufbewahren für	Aufbewahrungsdauer in Tagen für abgespielte/gelesene Sprachnachrichten Standardwert: 30
Gespeicherte Nachrichten aufbewahren für	Aufbewahrungsdauer in Tagen für gespeicherte Sprachnachrichten Standardwert: 365
Gelöschte Nachrichten aufbewahren für	Aufbewahrungsdauer in Tagen für gelöschte Sprachnachrichten Standardwert: 30
Faxnr.	
Faxnachrichten im Posteingang aufbewahren für	Aufbewahrungsdauer in Tagen für Faxnachrichten im Posteingang Standardwert: 30
Gelesene Faxnachrichten aufbewahren für	Aufbewahrungsdauer in Tagen für gelesene Faxnachrichten Standardwert: 30
Gelöschte Faxnachrichten aufbewahren für	Aufbewahrungsdauer in Tagen für gelöschte Faxnachrichten Standardwert: 30
Gesendete Faxnachrichten aufbewahren für	Aufbewahrungsdauer in Tagen für gesendete Faxnachrichten Standardwert: 30
Wartung der Anrufinformationen	
Anrufhistorie aufbewahren für	Aufbewahrungsdauer in Tagen für Anrufe im Journal Standardwert: 30
Contact Center	Aufbewahrungsdauer in Tagen für die mit myAgent aufgezeichneten Anrufe und die empfangenen und gesendeten Faxe und E-Mails für das Contact Center Standardwert: 30
Wartung der Protokolldateien	

Parameter	Beschreibung
Protokollinformationen aufbewahren für	Aufbewahrungsdauer in Tagen für Protokolldateien Standardwert: 10
Berichte	
Kennwort zurücksetzen	Zurücksetzen des myReports-Administrator-Kennworts auf das Standardkennwort
Sprachnachrichten	
VoiceMail-Sprache	Voreinstellung der Sprache für das Menü und die systemeigenen Ansagen der Sprachbox
Wiedergabereihenfolge für Sprachnachrichten	Definition der Wiedergabereihenfolge für Sprachnachrichten Standardwert: Neueste zuerst
Wiedergabereihenfolge für Sprachnachrichten: Neueste zuerst	Die neueste Sprachnachricht wird zuerst angeboten.
Wiedergabereihenfolge für Sprachnachrichten: Älteste zuerst	Die älteste Sprachnachricht wird zuerst angeboten.
Aufzeichnungszeit Sprachnachricht	Definition der maximalen Aufzeichnungsdauer für eine Sprachnachricht in Sekunden Standardwert: 900
VoiceMail-Modus	Definition des Funktionsumfangs der Sprachbox Standardwert: Voll
VoiceMail-Modus: Voll	Voller Funktionsumfang für die Sprachbox
VoiceMail-Modus: Kurzmenü	Nach der statusbezogenen oder persönlichen Ansage wird das Verbinden zum Empfang angeboten.
VoiceMail-Modus: Kein VoiceMail-Menü	Nach der Begrüßungsansage wird der Anrufer direkt zur Sprachaufzeichnung weitergeleitet.
Rückruf von VM nur an bekannte Nummer zulassen	Bei aktiviertem Flag wird der Zugriff von Anrufern auf die Sprachbox verhindert, deren Rufnummern nicht im UC Client hinterlegt sind. Standardwert: Aktiviert

27.4.3.14 OpenScape Business UC Suite > Profile

Parameterbeschreibung der Registerkarten:

- **Hinzufügen / Bearbeiten**

Parameter	Beschreibung
Profile	Benutzer-Profile speichern Einstellungen von Benutzern der UC Suite. Einem Benutzer-Profil können mehrere Benutzer (Mitglieder) zugeordnet werden. Alle Mitglieder dieses Profils haben (zunächst) die gleichen Einstellungen. Es können mehrere Profile erstellt werden, die für verschiedene Benutzergruppen unterschiedliche Voreinstellungen ermöglichen.
Name	Name des Profils (freie Eingabe)

Parameterbeschreibung der Registerkarten:

- **Benutzer zuordnen**

Parameter	Beschreibung
Benutzer	Benutzer, für welche das Profil gelten soll
Persönliche Daten	
Eigene persönliche Daten	Ausgewählte persönliche Daten für die zugeordneten Benutzer. Das Schlosssymbol legt fest, ob der Benutzer diese Einstellungen selbst ändern kann.
Meine Einstellungen	
Darstellung	Skin und Sprache des UC Clients der zugeordneten Benutzer. Das Schlosssymbol legt fest, ob der Benutzer diese Einstellungen selbst ändern kann.
Benachrichtigung	Benachrichtigungen für die zugeordneten Benutzer. Das Schlosssymbol legt fest, ob der Benutzer diese Einstellungen selbst ändern kann.
Outlook-Anbindung	Kalenderintegration für die zugeordneten Benutzer. Das Schlosssymbol legt fest, ob der Benutzer diese Einstellungen selbst ändern kann.
Verschiedenes	Automatische Rückkehr zum Anwesenheitsstatus "Büro", Übergabemethode und Aufbewahrungsdauer des Anrufjournals für die zugeordneten Benutzer. Das Schlosssymbol legt fest, ob der Benutzer diese Einstellungen selbst ändern kann.
Anrufregeln	
Anrufweiterleitungsziele	Weiterleitungsziele für kommende Anrufe in Abhängigkeit vom Anwesenheitsstatus für die zugeordneten Benutzer. Das Schlosssymbol legt fest, ob der Benutzer diese Einstellungen selbst ändern kann.
Kommunikation	
Einstellungen für Sprachnachrichten	Aufzeichnung von Sprachnachrichten in Abhängigkeit vom Anwesenheitsstatus für die zugeordneten Benutzer. Das Schlosssymbol legt fest, ob der Benutzer diese Einstellungen selbst ändern kann.
Sprachnachricht-Benachrichtigung	Mitteilung bei neuen Sprachnachrichten für die zugeordneten Benutzer. Das Schlosssymbol legt fest, ob der Benutzer diese Einstellungen selbst ändern kann.
Fax-Benachrichtigung	Mitteilung bei neuen Faxnachrichten für die zugeordneten Benutzer. Das Schlosssymbol legt fest, ob der Benutzer diese Einstellungen selbst ändern kann.
Profile	
Profile	Persönlicher AutoAttendant für die zugeordneten Benutzer. Die betreffenden Benutzer müssen eine Ansage zur Auswahl aufzeichnen. Das Schlosssymbol legt fest, ob der Benutzer diese Einstellungen selbst ändern kann.
Sensibilität	
Sicherheit und Zugriff	Abhören von Sprachnachrichten mit myAttendant zulassen sowie Abfrage der Sprachbox vom eigenen Telefon ohne Kennwort. Das Schlosssymbol legt fest, ob der Benutzer diese Einstellungen selbst ändern kann.
Sichtbarkeit des Anwesenheitsstatus	Interne Teilnehmer, welche den Anwesenheitsstatus sehen dürfen. Das Schlosssymbol legt fest, ob der Benutzer diese Einstellungen selbst ändern kann.
VoiceMail-Anwesenheitsstatus	Interne bzw. externe Anrufer, welche über den Anwesenheitsstatus durch automatische Ansagen der Sprachbox informiert werden sollen. Das Schlosssymbol legt fest, ob der Benutzer diese Einstellungen selbst ändern kann.

27.4.3.15 OpenScape Business UC Suite > Faxkopfzeilen

Parameterbeschreibung der Registerkarten:

- **Bearbeiten**
- **Hinzufügen**
- **Entfernen**

Parameter	Beschreibung
ID	ID, mit welcher die Kopfzeile in Fax Printer zur Auswahl angezeigt wird
Name	Name der Kopfzeile (muss eindeutig sein).
Text	Platzhalter für Datum/Uhrzeit, Firmenname, Benutzername, Firmen-Rufnr., Seitennummer sowie Anzahl der Seiten können eingefügt werden.

27.4.3.16 OpenScape Business UC Suite > Skin-Einstellungen

Parameterbeschreibung der Registerkarten:

- **Skin-Einstellungen**

Parameter	Beschreibung
Browse	Navigation zum Ablageort der Datei mit den zu ladenden Skin-Einstellungen.
Upload	Lädt die Datei mit den Skin-Einstellungen.
Löschen	Löscht die Datei mit den Skin-Einstellungen..

27.4.4 Web Services

Unter **Web Services** sind die Funktionen für die Konfiguration der Web-Schnittstellen zusammengefasst, wie z . B. zu Web Collaboration.

27.4.4.1 Web Services > XMPP

Parameterbeschreibung der Registerkarten:

- **XMPP Parameter ändern**

Parameter	Beschreibung
XMPP Modus ein	XMPP aktivieren
XMPP-Stand-alone	Die Anlage ist ein Standalone-System

Parameter	Beschreibung
XMPP in der Vernetzung	Die Anlage ist in einem Netzwerk
XMPP Domäne	Angabe der Website unter der das System im Internet erreichbar ist. In Form von: oso.examplefor-a-domain.com.
Sichere Verbindungen (TLS) zulassen	Nur gesicherte Verbindungen zu anderen Servern benutzen

27.4.4.2 Web Services > Web Collaboration

Für die Einbindung der Web Collaboration über einen Public Server (Web Collaboration Server als Dienst im Internet) oder über einen Custom Server (Web Collaboration Server im Kundennetz oder bei einem Partner). Web Collaboration ist nur in Verbindung mit UC Suite möglich.

Parameterbeschreibung der Registerkarten:

- **Web Collaboration Server**

Parameter	Beschreibung
Server Typ	Auswahl des Web Collaboration Servers.
Server Typ: **Public Server**	Der Web Collaboration Server ist ein Public Server und befindet sich im Internet. Dafür wird eine gesicherte https-Verbindung verwendet. Zusätzlich wird eine Lizenznummer und ein Passwort benötigt. Standardmäßig wird der TCP-Port 5100 verwendet.
Server Typ: **Public Server (Demo Mode/Evaluation Mode)**	Die Web Collaboration kann 5 min lang getestet werden. Dafür ist keine Eingabe von IP-Adresse, Lizenznummer und Passwort nötig.
Server Typ: **Custom Server**	Der Web Collaboration Server ist ein Custom Server und befindet sich im Kundennetz oder bei einem Partner. Dafür kann eine gesicherte https-Verbindung oder eine ungesicherte http-Verbindung verwendet werden. Bei Verbindung über https wird zusätzlich eine Lizenznummer und ein Passwort benötigt. Standardmäßig wird der TCP-Port 5004 verwendet.
Server Typ: **Kein Web Collaboration Server**	Es wird kein Web Collaboration Server verwendet. Die Option zum Starten einer Web Collaboration Sitzung ist in den UC Clients deaktiviert.

URL / IP-Adresse	Eingabe der URL / IP-Adresse des entsprechenden Web Collaboration Servers. Public Server über https und Custom Server über https oder http.
	Beispiel:
	`http://<Webcollaboration Server IP Adresse>:5004/OscInterface`
	`https://<Webcollaboration Server IP Adresse>:5100/XMLRPSecure`

Lizenznummer	Lizenznummer für die Verbindung zum Web Collaboration Server.
Passwort	Passwort für die Verbindung zum Web Collaboration Server.

27.4.5 Open Directory Service

Unter **Open Directory Service** sind die Funktionen für die Konfiguration von Open Directory Service zusammengefasst.

27.4.5.1 Open Directory Service > Grundeinstellungen

Parameter	Beschreibung
Aktivieren/Deaktivieren des Open Directory Service	Standardwert: deaktiviert
LDAP-Server Login-Daten	Login-Daten des externen Datenbankservers. Open Directory Service muss berechtigt sein, auf die externe Datenbank zuzugreifen, ggf. muss in dem Server ein eigener Benutzer hinzugefügt werden.

27.4.5.2 Open Directory Service > Datenquellen > OpenScape Business

Parameterbeschreibung der Registerkarten:

- **Überblick über die konfigurierten Datenquellen**

Parameter	Beschreibung
OpenScape Office Verzeichnisse	Internes Verzeichnis von UC Suite. Das Verzeichnis ist Open Directory Service fest zugeordnet und kann nicht gelöscht oder geändert werden.
Kurzwahlziele	Zentrale Kurzwahlnummern. Das Verzeichnis ist Open Directory Service fest zugeordnet und kann nicht gelöscht oder geändert werden.
Hinzufügen	Externe Datenquellen für Kontaktdaten aus Datenbanken mit lesendem Zugriff via ODBC

Parameterbeschreibung der Registerkarten:

- **Bearbeitete Datenquelle**

Parameter	Beschreibung
Neue Datenquelle	Parameter der hinzugefügten Datenquellen können hier geändert werden

27.4.5.3 Open Directory Service > Datenquellen > Kurzwahlen

Parameter	Beschreibung
Kurzwahlziele	Zentrale Kurzwahlnummern. Das Verzeichnis ist Open Directory Service fest zugeordnet und kann nicht gelöscht oder geändert werden.

27.4.5.4 Open Directory Service > Datenquellen > LXV3

Parameter	Beschreibung
Überblick über die konfigurierten Datenquellen	Eine LDAP-Ausgabezuordnung legt fest, welche der Felder des Datenschemas von Open Directory Service via LDAP ausgegeben werden sollen. Beispiel: für spezifische LDAP-Clients oder für verschiedene Gruppen von Teilnehmern, welche nicht alle Details sehen sollen, sondern nur eine definierte Untermenge. Die LDAP-Ausgabezuordnung web steht standardmäßig zur Verfügung und kann nicht gelöscht oder geändert werden. In ihr sind alle Felder des Datenschemas von Open Directory Service der LDAP-Ausgabe fest zugeordnet. Sie können weitere LDAP-Ausgabezuordnungen konfigurieren.
Hinzufügen	Weitere Ausgabezuordnungen hinzufügen. Über den Parameter dc im LDAP-Login können LDAP-Clients auf eine bestimmte LDAP-Ausgabezuordnung zugreifen, z. B.: dc=web.

27.4.5.5 Open Directory Service > Wartung

Parameterbeschreibung der Registerkarten:

- **Wartung**

Parameter	Beschreibung
Open Directory Service prüfen / neu starten	Statusanzeige des Open Directory Service (grau = deaktiviert, rot = Konfiguration fehlerhaft oder Datenquelle nicht verfügbar, grün = aktiviert)
Neustart	Neustart des Open Directory Service

27.4.5.6 OpenStage Gate View

Unter **OpenStage Gate View** kann OpenStage Gate View aktiviert oder deaktiviert werden und die OpenStage Gate View Server-Software gestartet werden.

27.4.6 OpenStage Gate View

Parameter	Beschreibung
Aktivieren	OpenStage Gate View aktivieren.
Deaktivieren	OpenStage Gate View deaktivieren.
Anmelden	Aufrufen der OpenStage Gate View Server-Software.

27.4.7 Application Launcher

Unter **Application Launcher** sind die Funktionen für die Konfiguration von Application Launcher zusammengefasst.

27.4.7.1 Application Launcher

Parameter	Beschreibung
Hochladen der Konfigurationsdatei	Profil mit Konfigurationsdaten von Application Launcher zur schnellen Konfiguration von Application Launcher auf allen Client-PCs. Sobald Application Launcher für einen ersten Benutzer vollständig konfiguriert ist, können Sie als Administrator dessen Profil mit den Konfigurationsdaten von Application Launcher im Kommunikationssystem bereitstellen. Anschließend können alle Benutzer die Konfiguration von Application Launcher durch Importieren dieses Profils durchführen.
Profil	Erlaubter Dateityp .xml

27.4.8 IVM

Unter **IVM** wird die IP-Adresse der IVM (Xpressions Compact) und somit das webbasierte Konfigurationsmenü der IVM aufgerufen. Der Menüeintrag erscheint nur, wenn eine IVM im System installiert ist.

27.5 Middleware

Unter **Middleware** sind Funktionen für die Konfiguration der Middleware zusammengefasst.

27.5.1 Wiedergabegerät für Ansagen

Parameterbeschreibung der Registerkarten:

- **Einstellungen - Wiedergabegerät für Ansagen**
- **Statistiken - Wiedergabegerät für Ansagen**

Parameter	Beschreibung
Aktivierung	
Dienst wird automatisch gestartet	Aktivierung oder Deaktivierung des Wiedergabegeräts für Ansagen.
Statistiken - Wiedergabegerät für Ansagen	Hier wird der Status des Wiedergabegeräts dargestellt. Die Daten werden automatisch alle 5 Minuten aktualisiert. Die Seite kann aber auch manuell aktualisiert werden.

27.5.2 CSTA Message Dispatcher (CMD)

Parameterbeschreibung der Registerkarten:

- **Einstellungen - CSTA Message Dispatcher (CMD)**
- **Statistiken - CSTA Message Dispatcher (CMD)**

Parameter	Beschreibung
Aktivierung	
Dienst wird automatisch gestartet	Aktivierung oder Deaktivierung des CSTA Message Dispatchers (CMD). Der CMD stellt die Verbindung zwischen den OpenScape Business TAPI 120 Clients und dem Kommunikationssystem her und ist für die Funktionalität notwendig.
Autom. Registrierung	
Autom. Registrierung des Clients aktiv	Aktivierung oder Deaktivierung der automatischen Anmeldung der Clients. Automatische Anmeldung bedeutet, dass neue Einträge in der Liste der CTI-Firewall möglich sind. Dadurch wird die CTI-Firewall automatisch konfiguriert. Haben sich alle berechtigten Clients angemeldet, kann das Häkchen entfernt werden und neue Einträge in die CTI-Firewall werden verhindert. Ein PC kann berechtigt werden, eine bestimmte Nebenstelle zu kontrollieren. Die TAPI/CTI-Lizenzen müssen zusätzlich vergeben werden.
CTI-Firewall	
Löschen	Einträge mit einem Häkchen in der Löschen-Spalte werden aus der Liste der berechtigten Clients entfernt, sobald auf die Schaltfläche **Übernehmen** geklickt wird. Eine Anmeldung wird dann abgewiesen, sofern nicht die automatische Registrierung aktiv ist.
Anwendungs-ID	Name des PC, von dem aus eine Nebenstelle kontrolliert werden kann. Durch Verwendung des PC-Namens kann für die OpenScape Business TAPI 120 PCs auch DHCP verwendet werden.
Rufnummer	Interne Rufnummer der Nebenstelle, die kontrolliert werden darf.
Statistiken - CSTA Message Dispatcher (CMD)	Hier wird der Status des CMD dargestellt. Im laufenden Betrieb kann kontrolliert werden, welche OpenScape Business TAPI 120 mit dem CMD verbunden sind, dass evtl. Lizenzen zugewiesen werden müssen. Die Daten werden automatisch alle 5 Minuten aktualisiert. Die Seite kann aber auch manuell aktualisiert werden.

27.5.3 CSTA Service Provider (CSP)

Parameterbeschreibung der Registerkarten:

- **Einstellungen - CSTA Service Provider (CSP)**
- **Statistiken - CSTA Service Provider (CSP)**

Parameter	Beschreibung
Aktivierung	
Dienst wird automatisch gestartet	Aktivierung oder Deaktivierung des CSTA Service Providers (CSP). Der CSP wird für die UC-Suite, für den DSS-Server (Presence Manager, nur in Vernetzung), den OpenScape Business TAPI 170 und für externe CSTA-Applikationen benötigt.
CSTA-Zugang	
CSTA-Benutzer-ID / **CSTA-Benutzerpasswort**	OpenScape Business TAPI 170 und externe CSTA-Applikationen können sich nur mit den hier konfigurierten Benutzerkonto am CSP anmelden. Ist kein CSTA-Benutzer konfiguriert, ist die Verwendung von OpenScape Business TAPI 170 oder externen CSTA Applikationen am CSP nicht möglich.
Statistiken - CSTA Service Provider (CSP)	Hier wird der Status des CSP dargestellt. Man sieht wieviele und welche Applikationen mit dem CSP verbunden sind. Unbekannte Applikationen werden mit ‚Default' dargestellt. Der Verbindungsstatus zu den einzelnen Knoten des Netzwerks / dem lokalen Knoten kann eingesehen werden. Die Daten werden automatisch alle 5 Minuten aktualisiert. Die Seite kann aber auch manuell aktualisiert werden.

27.5.4 DSS-Server

Parameterbeschreibung der Registerkarten:

- **Einstellungen - DSS-Server**
- **Statistiken - DSS-Server**

Parameter	Beschreibung
Aktivierung	
Dienst wird automatisch gestartet	Aktivierung oder Deaktivierung des DSS-Servers.
Statistiken - DSS-Server	Hier wird der Status des DSS-Servers dargestellt. Die Daten werden automatisch alle 5 Minuten aktualisiert. Die Seite kann aber auch manuell aktualisiert werden.

27.5.5 Media Extension Bridge (MEB)

Parameterbeschreibung der Registerkarten:

- **Einstellungen - Media Extension Bridge (MEB)**
- **Statistiken - Media Extension Bridge (MEB)**

Parameter	Beschreibung
Aktivierung	
Dienst wird automatisch gestartet	Aktivierung oder Deaktivierung der Media Extension Bridge.
Statistiken - Media Extension Bridge (MEB)	Hier wird der Status des MEB dargestellt. Die Daten werden automatisch alle 5 Minuten aktualisiert. Die Seite kann aber auch manuell aktualisiert werden.

28 Anhang

Der Anhang enthält Referenzinformationen, wie zum Beispiel die unterstützten Sprachen, Standards, Ausbaugrenzen und Kapazitäten, Euro-ISDN-Leistungsmerkmale, Kennzahlen zur Aktivierung und Deaktivierung von Leistungsmerkmalen, Leistungsmerkmal-Codes über MFV und verwendete IP-Protokolle und Portnummern.

28.1 Unterstützte Standards

Hier erhalten Sie Informationen über die unterstützten Standards.

Ethernet

- RFC 894 Ethernet II Encapsulation
- IEEE 802.1Q Virtual LANs
- IEEE 802.2 Logical Link Control
- IEEE 802.3u 100BASE-T
- IEEE 802.3ab Gigabit Ethernet
- IEEE 802.3X Full Duplex Operation

IP / Routing

- RFC 768 UDP
- RFC 791 IP
- RFC 792 ICMP
- RFC 793 TCP
- RFC 2822 Internet Message Format
- RFC 826 ARP
- RFC 2131 DHCP
- RFC 1918 IP Addressing
- RFC 1332 The PPP Internet Protocol Control Protocol (IPCP)
- RFC 1334 PPP Authentication Protocols
- RFC 1618 PPP over ISDN
- RFC 1661 The Point-to-Point Protocol (PPP)
- RFC 1877 PPP Internet Protocol Control Protocol
- RFC 1990 The PPP Multilink Protocol (MP)
- RFC 1994 PPP Challenge Handshake Authentication Protocol (CHAP)
- RFC 2516 A Method for Transmitting PPP Over Ethernet (PPPoE)
- RFC 3544 IP Header Compression over PPP

NAT

- RFC 2663 NAT

IPSec

- RFC 2401 Security Architecture for IP
- RFC 2402 AH - IP Authentication Header
- RFC 2403 IPsec Authentication - MD5
- RFC 2404 IPsec Authentication - SHA-1
- RFC 2405 IPsec Encryption - DES
- RFC 2406 ESP - IPsec encryption
- RFC 2407 IPsec DOI
- RFC 2408 ISAKMP
- RFC 2409 IKE
- RFC 2410 IPsec encryption - NULL
- RFC 2411 IP Security Document Roadmap
- RFC 2412 OAKLEY

SNMP

- RFC 1213 MIB-II

QoS

- IEEE 802.1p Priority Tagging
- RFC 1349 Type of Service in the IP Suite
- RFC 2475 An Architecture for Differentiated Services
- RFC 2597 Assured Forwarding PHB Group
- RFC 3246 An Expedited Forwarding PHB (Per-Hop Behavior)

Services

- RFC 2597 Assured Forwarding PHB Group
- RFC 3246 An Expedited Forwarding PHB (Per-Hop Behavior)

Codecs

- G.711
- G.729

VoIP über SIP

- RFC 2198 RTP Payload for Redundant Audio Data
- RFC 2327 SDP Session Description Protocol
- RFC 2617 HTTP Authentication: Basic and Digest Access Authentication
- RFC 2782 DNS RR for specifying the location of services (DNS SRV)
- RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
- RFC 3261 SIP Session Initiation Protocol
- RFC 3262 Provisional Response Acknowledgement (PRACK) Early Media
- RFC 3263 SIP Locating Servers

- RFC 3264 An Offer/Answer Model with the Session Description Protocol
- RFC 3310 HTTP Digest Authentication
- RFC 3311 Session Initiation Protocol (SIP) UPDATE Method
- RFC 3323 A Privacy Mechanism for the Session Initiation Protocol (SIP)
- RFC 3325 Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks
- RFC 3326 The Reason Header Field for the Session Initiation Protocol (SIP)
- RFC 3489 STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)
- RFC 3515 The Session Initiation Protocol (SIP) Refer Method
- RFC 3550 RTP: Transport Protocol for Real-Time Applications
- RFC 3551 RTP Profile for Audio and Video Conferences with Minimal Control
- RFC 3581 An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing
- RFC 3891 The Session Initiation Protocol (SIP) Replaces Header

XMPP

- RFC 3920 Extensible Messaging and Presence Protocol (XMPP): Core
- RFC 3921 Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence

Andere

- RFC 959 FTP
- RFC 1305 NTPv3
- RFC 1951 DEFLATE

28.2 Euro-ISDN-Leistungsmerkmale

Die Euro-ISDN-Leistungsmerkmale können an jedem Euro-ISDN-Anschluss genutzt werden, wenn die vorhandene Hardware (z. B. Telefon oder ISDN-Karte) dafür ausgelegt ist. Die Leistungsmerkmale stehen entweder dauerhaft im Amt zur Verfügung oder werden per Kennzahl aktiviert/deaktiviert.

Die Verfügbarkeit der Leistungsmerkmale ist abhängig vom Netzanbieter. Einige der genannten Leistungsmerkmale sind kostenpflichtig.

Thema	Erklärung
Mehrfachrufnummer (MSN = Multiple Subscriber Number)	Jedem Mehrgeräteanschluss können mehrere Rufnummern zugeordnet werden. Die Zuordnung dieser Rufnummern zu den einzelnen Endgeräten kann der Anwender selber an den Endgeräten vornehmen.
Rufnummernübermittlung (CLIP = Calling Line Identification Presentation)	Die eigene Rufnummer wird zum angerufenen Teilnehmer übermittelt und erscheint z. B. im Display des Telefons oder wird bei Nichtabheben in der Anrufliste gespeichert. Falsche Rufnummern können nicht übermittelt werden. Allerdings kann die Durchwahl von TK-Anlagen nicht geprüft werden. Die Übermittlung der eigenen Rufnummer kann ständig oder fallweise unterdrückt werden.
Rufnummernunterdrückung (CLIR = Calling Line Identification Restriction)	Die Übermittlung der Rufnummer kann auch dauerhaft oder fallweise abgeschaltet werden. Die Rufnummern-Anzeige beim B-Teilnehmer ist dann nur noch bei speziell dafür vorgesehene Anschlüsse möglich (Notruf, Polizei, Feuerwehr).
Rufnummernidentifikation/ Fangen (MCID = Malicious Call Identification)	Der Angerufene kann den anonymen Anrufer über die Vermittlungsstelle identifizieren lassen, auch wenn die Rufnummernübermittlung abgeschaltet ist. Dieses Leistungsmerkmal ist kostenpflichtig.
Umstecken am Bus (TP = Terminal Portability)	Dieses Leistungsmerkmal ermöglicht es Ihnen während einer bestehenden Verbindung das verwendete ISDN-Endgerät an einer anderen ISDN-Dose anzuschließen und das Gespräch fortzuführen. Das Gespräch muss vor dem Umstecken geparkt werden.
Subadressierung (SUB = Subaddressing)	Diese Funktion kann kostenpflichtig zusätzlich zur normalen Rufnummer genutzt werden. Mit dieser Subadressierung kann abhängig vom Anrufer ein anrufbares Endgerät gesteuert werden (z. B. Programm auf dem PC).
Teilnehmer zu Teilnehmer Zeichengabe (UUS = User-to-User-Signaling)	Während des Verbindungsauf- und abbaus können über den D-Kanal Informationen ausgetauscht werden. Die Übertragung ist in beide Richtungen möglich.
Geschlossene Benutzergruppe (CUG = Closed User Group)	Ist dieses Leistungsmerkmal aktiviert, sind keine Gespräche außerhalb der Benutzergruppe möglich (außer den Notrufnummern 110 und 112). Allerdings können auch Anrufer von außen gesperrt werden.
Anrufumleitung bei Besetzt (CFB = Call Forwarding Busy)	Diese Anrufweiterschaltung leitet Anrufe bei Besetzt an jeden beliebigen, aber erreichbaren Telefonanschluss weiter. Die Anrufweiterschaltung wird in der Vermittlungsstelle durchgeführt. Beide Nutzkanäle bleiben dadurch frei.
Direkte Anrufumleitung (CFU = Call Forwarding Unconditional)	Diese Anrufweiterschaltung leitet Anrufe sofort an jeden beliebigen, aber erreichbaren Telefonanschluss weiter. Die Anrufweiterschaltung wird in der Vermittlungsstelle durchgeführt. Beide Nutzkanäle bleiben dadurch frei.

Thema	Erklärung
Verzögerte Anrufumleitung (CFNR = Call Forwarding No Reply)	Diese Anrufweiterschaltung leitet Anrufe nach 20 Sekunden (bei nicht Erreichen) an jeden beliebigen, aber erreichbaren Telefonanschluss weiter. Die Anrufweiterschaltung wird in der Vermittlungsstelle durchgeführt. Beide Nutzkanäle bleiben dadurch frei.
Anklopfen (CW = Call Waiting)	Während einer bestehenden Verbindung wird ein weiterer Anrufer signalisiert. Der Anrufer hört währenddessen das Freizeichen. Die anklopfende Verbindung kann angenommen, abgelehnt oder einfach nur ignoriert werden.
Makeln (Hold = Call Hold)	Während einer bestehenden Verbindung kann durch Rückfrage eine zweite Verbindung aufgebaut werden. Wird zwischen den beiden Verbindungen hin und her geschaltet, spricht man von Makeln. Der wartende Gesprächsteilnehmer kann das andere aktive Gespräch nicht mithören.
Dreierkonferenz (3PTY = Three Party Service)	Zwei bestehende Verbindungen können zusammengeschaltet werden. Dadurch ist eine Telefonkonferenz mit 3 Teilnehmern möglich.
Automatischer Rückruf bei Besetzt (CCBS = Completion of Calls to Busy Subscriber)	Ist ein angerufener Teilnehmer besetzt, so kann dieses Leistungsmerkmal aktiviert werden. Sobald der Anschluss dieses Teilnehmers wieder frei ist, erhält man ein Signal. Bei Abheben des Hörers wird die Verbindung aufgebaut.
Gebührenanzeige am Ende des Gesprächs (AOCE = Advice of Charge (End))	Auf Wunsch lassen sich die Gesprächsgebühren am Ende des Gesprächs anzeigen. Eventuelle Rabatte und Tarife werden dabei nicht berücksichtigt.
Gebührenanzeige während des Gesprächs (AOCD = Advice of Charge (During))	Auf Wunsch lassen sich die Gesprächsgebühren während des Gesprächs anzeigen. Eventuelle Rabatte und Tarife werden dabei nicht berücksichtigt.

28.3 Verwendete Ports

Die OpenScape Business Systemkomponenten nutzen verschiedene Ports, die bei Bedarf in der Firewall freigeschaltet werden müssen. Für die Ports der Webbased Clients (z. B. myPortal to go) muss ein Port Forwarding im Router eingerichtet werden.

INFO: Die in der u.a. Liste mit "O" gekennzeichneten Ports sind optional, d.h. sie sind nicht dauerhaft in der Firewall geöffnet (z. B. ist der TFTP-Port nur bei aktiviertem Gate View offen).

Beschreibung	TCP	UDP	Portnummer	OpenScape Business X	UC Booster Card	OpenScape Business S	UC Booster Server
Systemkomponenten							
Admin Portal (https)	X		443	X	X	X	X
CAR Update Registration	X		12061	X		X	

Beschreibung	TCP	UDP	Portnummer	OpenScape Business X	UC Booster Card	OpenScape Business S	UC Booster Server
CAR Update Server	X		12063	X		X	
CLA	X		61740	O		O	O
CLA Auto Discovery		X	23232	X		X	X
CSTA Message Dispatcher (CMD)	X		8900		X	X	X
CSTA Protocol Handler (CPH)	X		7004	X		X	
CSTA Service Provider (CSP)	X		8800		X	X	X
DHCP		X	67	X			
DLI	X		18443	X		X	X
DLSC	X		8084	X		X	X
DNS	X	X	53	X			
FTP	X		21	O		O	
FTP Passive	X		40000:40040	O		O	
Gate View	X		8000:8010		O	O	O
HFA	X		4060	X		X	
HFA Secure	X		4061	X		X	
JSFT	X		8771		X	X	X
JSFT	X		8772		X	X	X
LAS Cloud Service	X		8602	X			
LDAP Server	X		389		X	X	X
Manager E	X		7000	X			
MEB SIP	X		15060		X		X
NAT traversal (NAT-T)		X	4500	X			
NTP		X	123	X			
Openfire Admin (https)	X		9091		X	X	X
OSBiz Multisite	X		8778		X	X	X
OSBiz myReports (http)	X		8101		X	X	X
OSBiz Status Server	X		8808	X		X	X
OSBiz User Portal	X	X	8779		X	X	X
Postgres	X		5432	X	X	X	X
RTP		X	29100:30530	X	X	X	X
SIP (server)	X	X	5060	X		X	
SIP TLS SIPQ (server)	X		5061	X		X	

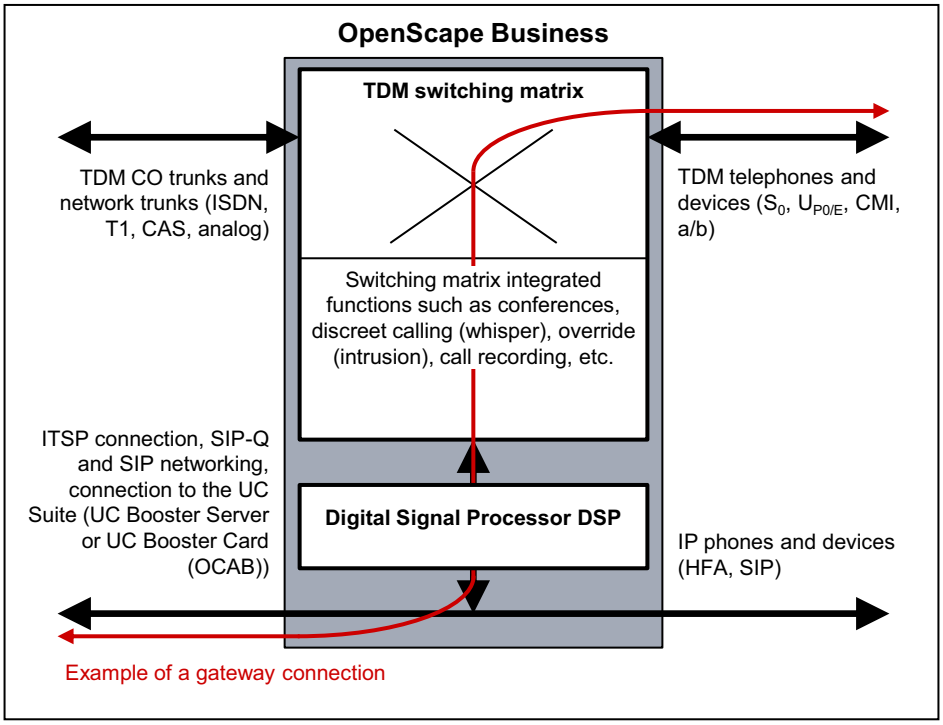
Beschreibung	TCP	UDP	Portnummer	OpenScape Business X	UC Booster Card	OpenScape Business S	UC Booster Server
SIP TLS Subscriber (server)	X		5062	X		X	
SNMP (Get/Set)		X	161	X		X	
SNMP (Traps)		X	162	X		X	
SSDP	X		3011	X		X	X
TFTP		X	69		O	O	O
VSL	X		8770		X	X	X
Webadmin for Clients	X		8803	X	X	X	X
XMPP Connection Manager	X		5262		X	X	X
XMPP Server	X		5269		X	X	X
Webbased Clients							
Webbased Clients (http)	X		8801	X	X	X	X
Webbased Clients (https)	X		8802	X	X	X	X

INFO: Aus Sicherheitsgründen wird empfohlen für die Webbased Clients ausschließlich https zu verwenden und ein Port Forwarding von extern TCP/443 nach intern TCP/8802 einzurichten.

28.4 Projektierung der DSP-Kanäle für die Kommunikationssysteme OpenScape Business X3/X5/X8

Verbindungen zwischen IP- und TDM-Telefonen/-Leitungen sind sogenannte Gateway-Verbindungen, für die jeweils ein DSP (Digital Signal Processor)-Kanal benötigt wird. Darüber hinaus werden DSP-Kanäle bei Aktivierung des Leistungsmerkmals Signaling And Payload Encryption SPE benötigt.

Keine DSP-Kanäle werden für reine TDM-Verbindungen und für reine IP-Verbindungen benötigt.



Die Mainboards der Kommunikationssysteme OpenScape Business X3/X5/X8 stellen maximal acht DSP-Kanäle zur Verfügung.

Reichen die DSP-Kanäle eines Mainboards nicht aus, können weitere Kanäle durch das Stecken einer Voice Channel Booster Card (Submodul OCCB1 oder OCCB3) bereitgestellt werden:

- OCCB1 stellt bis zu 40 zusätzliche DSP-Kanäle zur Verfügung.
- OCCB3 stellt maximal 120 zusätzliche DSP-Kanäle zur Verfügung.

Die Anzahl der für Gateway-Verbindungen zur Verfügung stehenden DSP-Kanäle verringert sich durch die Verwendung des Codecs G.729 und durch die Nutzung von Signaling And Payload Encryption SPE.

Letztendlich bestimmt die Anzahl der gleichzeitigen Gateway-Verbindungen (der gleichzeitigen Sprachverbindungen mit IP-TDM-Übergang), ob ein OCCB-Submodul und welches OCCB-Submodul einzusetzen ist.

> ***INFO:*** Angaben zu den maximal zur Verfügung stehenden DSP-Kanälen der Mainboards und der OCCB-Submodule, siehe Systembedingte Ausbaugrenzen.

Bei einer Unterdimensionierung von DSP-Kanälen kann es zu DSP-Engpässen kommen, die sich beispielsweise durch Besetztzustände beim Verbindungsaufbau äußern (Besetztton beim Verbindungsaufbau, Displayanzeige `Zur Zeit nicht möglich`).

Bei Auftreten eines DSP-Engpasses erfolgt ein Eintrag in der Event-Protokolldatei (Event Log) des Kommunikationssystems.

Folgende Maßnahmen sind bei häufigem Auftreten von DSP-Engpässen zu ergreifen:

Wenn	Dann
Die DSP-Kanäle des Mainboards werden genutzt.	Submodul OCCB1 oder OCCB3 auf dem Mainboard einsetzen.
Die DSP-Kanäle des Mainboards und des Submoduls OCCB1 werden genutzt.	Submodul OCCB3 auf dem Mainboard einsetzen.
Die DSP-Kanäle des Mainboards und des Submoduls OCCB3 werden genutzt.	Zu prüfen ist, ob das Kommunikationssystem ausschließlich mit Codec G.711 betrieben werden kann. Dadurch erhöht sich die Anzahl der DSP-Kanäle auf das Maximum. ***INFO:*** Die Option **Ausschließlich G.711 verwenden** kann durch einen Administrator mit dem Profil **Expert** über den **Experten-Modus** (**Telefonie > Sprachgateway > Codec-Parameter**) aktiviert werden.

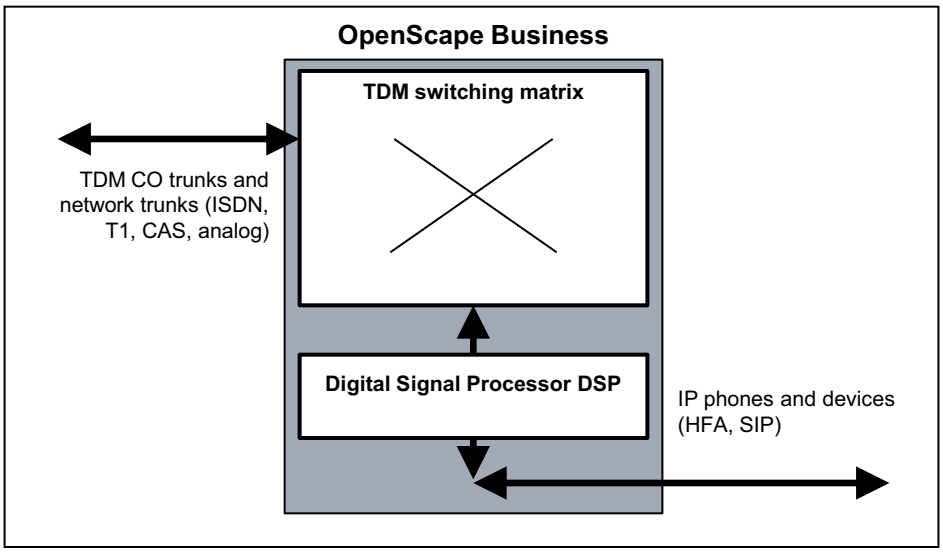
Die folgende Tabelle liefert Orientierungswerte, ob und welches OCCB-Submodul einzusetzen ist.

Summe der TDM-Kanäle: Amts- und Vernetzungsleitungen (ISDN, T1, CAS, analog)	Summe der IP-Kanäle: ITSP-Anschaltung, SIP-Q- und SIP-Vernetzung, Verbindung zur UC Suite (UC Booster Server oder UC Booster Card (OCAB))	Summe der TDM-Telefone und TDM-Geräte (S_0, $U_{P0/E}$, CMI, a/b)	Summe der IP-Telefone und IP-Geräte (HFA, SIP)	Welches OCCB-Submodul?	Hinweise
beliebig viele	Ansagen (bis zu 16) 0	beliebig viele	0	kein OCCB-Submodul	Smart VM und Systemkonferenzen werden durch das Koppelfeld verarbeitet.
			bis 8	kein OCCB-Submodul	Unabhängig von den TDM-Kanälen Smart VM und Systemkonferenzen in Kombination mit IP-Telefonen und IP-Geräten benötigen DSP-Ressourcen.
			9 bis 100	OCCB1	dito, bis 40 gleichzeitig

Summe der TDM-Kanäle: Amts- und Vernetzungs-leitungen (ISDN, T1, CAS, analog)	Summe der IP-Kanäle: ITSP-Anschaltung, SIP-Q- und SIP-Vernet-zung, Verbin-dung zur UC Suite (UC Booster Ser-ver oder UC Booster Card (OCAB))	Summe der TDM-Telefone und TDM-Geräte (S_0, $U_{P0/E}$, CMI, a/b)	Summe der IP-Telefone und IP-Geräte (HFA, SIP)	Welches OCCB-Sub-modul?	Hinweise
			> 100	OCCB3	dito, bis 120 gleichzeitig
	> 0	bis 8		kein OCCB-Submodul	
	> 0	9 bis 100		OCCB1	bis 40 gleichzeitig
	> 0	> 100		OCCB3	bis 120 gleichzei-tig
> 0	bis 8			kein OCCB-Submodul	Kombination ist im wesentlichen bei SIP-Q und UC Suite relevant.
> 0	9 bis 40			OCCB1	dito
> 0	> 40			OCCB3	dito

Die folgenden Beispiele liefern Orientierungswerte, ob und welches OCCB-Submodul einzusetzen ist.

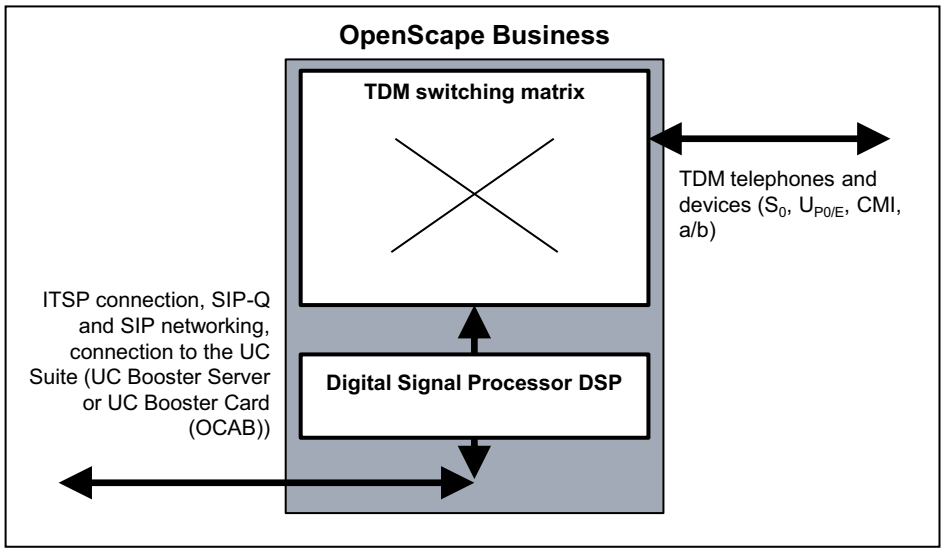
Beispiel 1: OpenScape Business mit TDM-Amtsleitungen und IP-Telefonen und -Geräten



Wenn	Dann
OpenScape Business mit: • 1 x TDM-Amt (ISDN) • 20 x IP-Telefon (HFA, SIP)	Die DSP-Kanäle des Mainboards reichen aus. Kein OCCB-Submodul erforderlich.
OpenScape Business mit: • 1 x TDM-Amt (ISDN) • 100 x IP-Telefon (HFA, SIP)	Submodul OCCB1 ist erforderlich. Alternativ kann Submodul OCCB3 eingesetzt werden.
OpenScape Business mit: • 2 x TDM-Amt (ISDN) • 100 x IP-Telefon (HFA, SIP)	Submodul OCCB3 ist erforderlich.
OpenScape Business mit: • 4 x TDM-Amt (ISDN) • 500 x IP-Telefon (HFA, SIP)	Submodul OCCB3 ist erforderlich. ***HINWEIS:*** Bei diesem Systemausbau darf ausschließlich der Codec G.711 verwendet werden, um die maximale Anzahl der DSP-Kanäle zu erreichen.

Soll das Kommunikationssystem auch mit TDM-Telefonen und -Geräten (S_0, $U_{P0/E}$, CMI, a/b) ausgestattet werden, sind dafür zusätzliche DSP-Kanäle zu berücksichtigen.

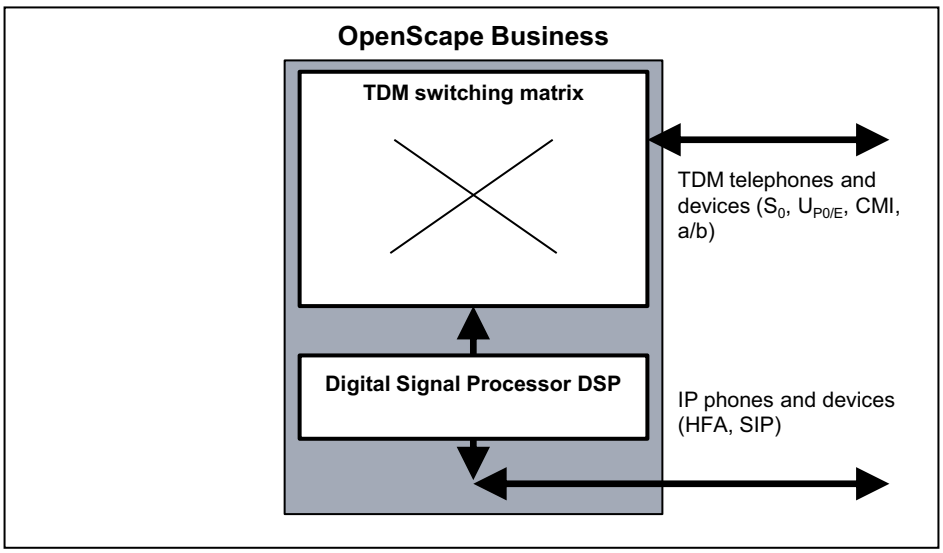
Beispiel 2: OpenScape Business mit ITSP-Anschaltung und TDM-Telefonen und -Geräten



Wenn	Dann
OpenScape Business mit: • 6 x ITSP-Anschaltung (6 B-Kanäle) • 20 x TDM-Telefon (S_0, $U_{P0/E}$, CMI, a/b)	Die DSP-Kanäle des Mainboards reichen aus. Kein OCCB-Submodul erforderlich.
OpenScape Business mit: • 30 x ITSP-Anschaltung (30 B-Kanäle) • 100 x TDM-Telefon (S_0, $U_{P0/E}$, CMI, a/b)	Submodul OCCB1 ist erforderlich. Alternativ kann Submodul OCCB3 eingesetzt werden.

Soll das Kommunikationssystem auch mit IP-Telefonen und -Geräten (HFA, SIP) ausgestattet werden, sind dafür zusätzliche DSP-Kanäle zu berücksichtigen.

Beispiel 3: OpenScape Business mit TDM-Telefonen und -Geräten und IP-Telefonen und Geräten



Wenn	Dann
OpenScape Business mit: • 6 x TDM-Telefon (S_0, $U_{P0/E}$, CMI, a/b) • 6 x IP-Telefon (HFA, SIP)	Die DSP-Kanäle des Mainboards reichen aus. Kein OCCB-Submodul erforderlich.
OpenScape Business mit: • 100 x TDM-Telefon (S_0, $U_{P0/E}$, CMI, a/b) • 100 x IP-Telefon (HFA, SIP)	Submodul OCCB3 ist erforderlich.

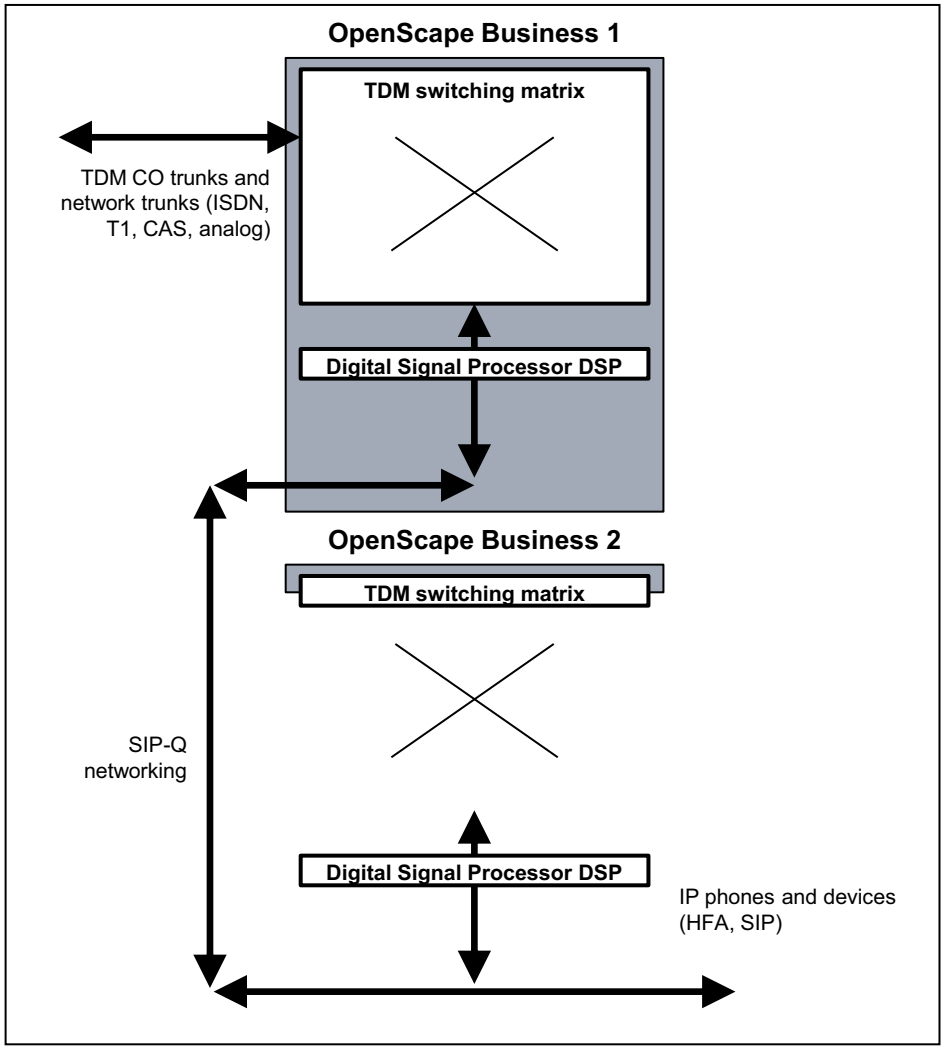
Soll das Kommunikationssystem auch mit TDM-Leitungen oder IP-Leitungen ausgestattet werden, sind dafür zusätzliche DSP-Kanäle zu berücksichtigen.

Beispiel 4: SIP-Q-Vernetzung OpenScape Business

Kommunikationssystem OpenScape Business 1 fungiert als Gateway zum TDM-Amt.

Ausschließlich am Kommunikationssystem OpenScape Business 2 sind IP-Telefone (HFA, SIP) angeschlossen.

In Abhängigkeit von der Anzahl der IP-Telefone am Kommunikationssystem OpenScape Business 2 sind die DSP-Kanäle für das Kommunikationssystem OpenScape Business 1 zu projektieren. DSP-Kanäle werden ausschließlich im TDM-Gateway benötigt.



Wenn	Dann
OpenScape Business 1 mit: • 1 x TDM-Amt (ISDN) OpenScape Business 2 mit: • 100 x IP-Telefon (HFA, SIP)	Submodul OCCB1 ist in OpenScape Business 1 erforderlich. Alternativ kann Submodul OCCB3 eingesetzt werden. Kein OCCB-Submodul in OpenScape Business 2 erforderlich.
OpenScape Business 1 mit: • 2 x TDM-Amt (ISDN) OpenScape Business 2 mit: • 100 x IP-Telefon (HFA, SIP)	Submodul OCCB3 ist in OpenScape Business 1 erforderlich. Kein OCCB-Submodul in OpenScape Business 2 erforderlich.
OpenScape Business 1 mit: • 4 x TDM-Amt (ISDN) OpenScape Business 2 mit: • 500 x IP-Telefon (HFA, SIP)	Submodul OCCB3 ist in OpenScape Business 1 erforderlich. ***HINWEIS:*** Bei diesem Systemausbau darf ausschließlich der Codec G.711 verwendet werden, um die maximale Anzahl der DSP-Kanäle zu erreichen. Kein OCCB-Submodul in OpenScape Business 2 erforderlich.

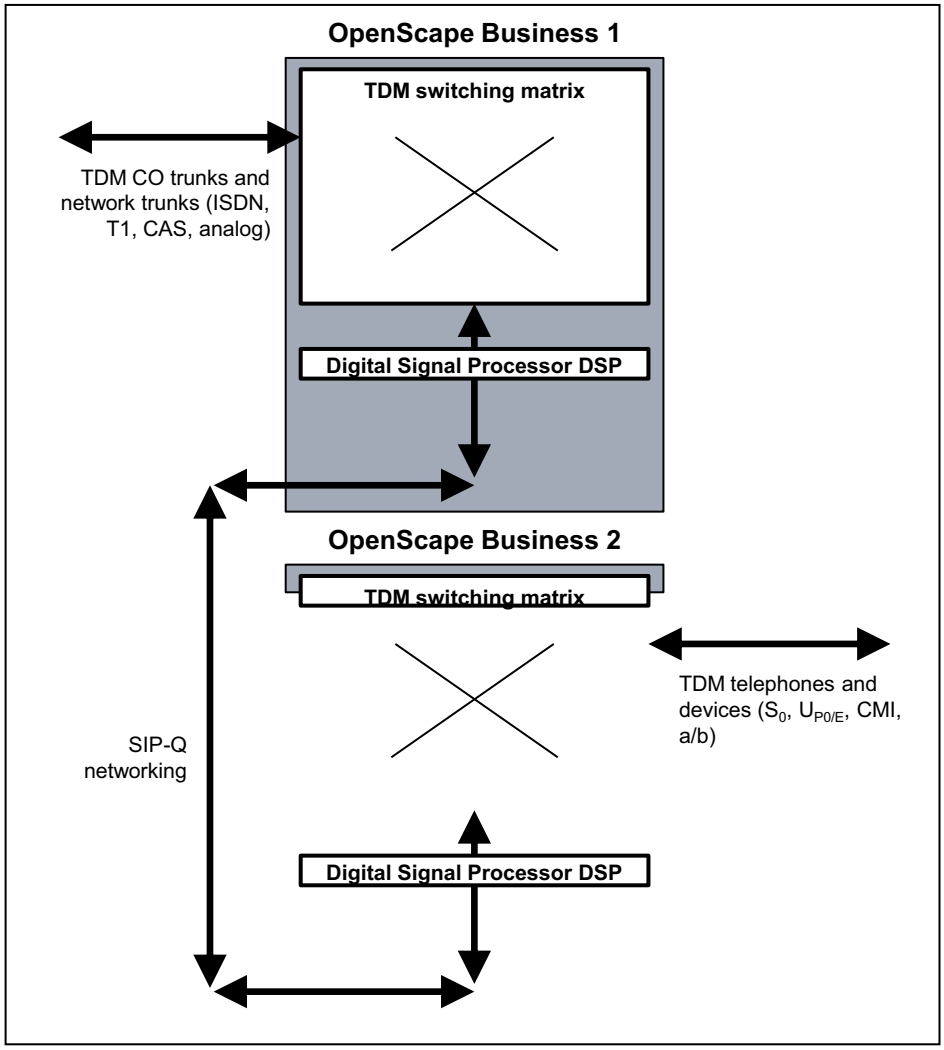
Soll das Kommunikationssystem OpenScape Business 2 auch mit TDM-Leitungen oder TDM-Telefonen und -Geräten (S_0, $U_{P0/E}$, CMI, a/b) ausgestattet werden, sind dafür zusätzliche DSP-Kanäle zu berücksichtigen.

Beispiel 5: SIP-Q-Vernetzung OpenScape Business

Kommunikationssystem OpenScape Business 1 fungiert als Gateway zum TDM-Amt.

Ausschließlich am Kommunikationssystem OpenScape Business 2 sind TDM-Telefon (S_0, $U_{P0/E}$, CMI, a/b) angeschlossen.

Da in beiden Kommunikationssystemen Gateway-Verbindungen (OpenScape Business 1: TDM-Amt <-> SIP-Q-Vernetzung, OpenScape Business 2: SIP-Q-Vernetzung <-> TDM-Telefon) erforderlich sind, werden in beiden Systemen DSP-Kanäle benötigt.



Wenn	Dann
OpenScape Business 1 mit: • 1 x TDM-Amt (ISDN) OpenScape Business 2 mit: • 100 x TDM-Telefon (S_0, $U_{P0/E}$, CMI, a/b)	Submodul OCCB1 ist in OpenScape Business 1 und in OpenScape Business 2 erforderlich. Alternativ kann jeweils Submodul OCCB3 eingesetzt werden.
OpenScape Business 1 mit: • 2 x TDM-Amt (ISDN) OpenScape Business 2 mit: • 100 x TDM-Telefon (S_0, $U_{P0/E}$, CMI, a/b)	Submodul OCCB3 ist in OpenScape Business 1 und in OpenScape Business 2 erforderlich.

Soll das Kommunikationssystem OpenScape Business 1 auch mit TDM-Telefonen und -Geräten (S_0, $U_{P0/E}$, CMI, a/b) ausgestattet werden, sind dafür zusätzliche DSP-Kanäle zu berücksichtigen.

29 Glossar

Das Glossar gibt kurze Erläuterungen zu verwendeten Begriffen (z. B. für Protokolle und Standards).

29.1 Glossar

10BaseT, 100BaseT, 1000BaseT

Hierbei handelt es sich um eine Spezifikation (IEEE 802.3i) für Netzwerke mit 10 MBit/s Basisbandübertragung über ein symmetrisches 100 Ohm Vierdrahtkabel. Dagegen steht 100BaseT für eine Bandbreite von bis zu 100 MBit/s und 1000BaseT für eine Bandbreite von bis zu 1000 MBit/s.

AES (Advanced Encryption Standard)

AES ist ein symmetrisches Kryptosystem, das als Nachfolger für DES bzw. 3DES vom National Institute of Standards and Technology als Standard bekannt gegeben wurde. Wird z. B. bei VPN verwendet.

ADSL mit dynamischer IP-Adresse

ADSL steht für Asymmetric Digital Subscriber Line und bedeutet, dass die Bandbreiten vom Internet (Download, Downstream) und zum Internet (Upload, Upstream) verschieden sind. ADSL entspricht dem klassischen DSL-Anschluss. Eine dynamische IP-Adresse ist ausreichend, wenn Sie die Web- und Email-Dienste vom Internet-Service-Provider bereitgestellt bekommen.

ADSL mit fester IP-Adresse

ADSL steht für Asymmetric Digital Subscriber Line und bedeutet, dass die Bandbreiten vom Internet (Download, Downstream) und zum Internet (Upload, Upstream) verschieden sind. ADSL entspricht dem klassischen DSL-Anschluss. ADSL mit fester IP-Adresse ist erforderlich, falls Sie eigene Web- und Email-Server an ihrem Standort betreiben möchten.

AF-EF (Expedited Forwarding - Assured Forwarding)

Die Codepunkte AF und EF legen die unterschiedlichen Priorisierungen von IP-Paketen bei QOS (Quality of Service) fest.

AF: Garantiert eine minimale Bandbreite für die Daten.

EF: Garantiert eine konstante Bandbreite für die Daten.

ARP (Address Resolution Protocol)

ARP ist ein Netzwerkprotokoll, das die Zuordnung von Netzwerkadressen zu Hardwareadressen möglich macht. Obwohl es nicht auf Ethernet- und IP-Protokolle beschränkt ist, wird es fast ausschließlich im Zusammenhang mit IP-Adressierung auf Ethernet-Netzen verwendet.

Authentication (Authentifizierung)

Authentication ist die Überprüfung der Identität einer Person oder eines PCs. Die Überprüfung kann mit einem einfachen Benutzernamen, aber z. B. auch mittels Fingerabdruck durchgeführt werden.

Authorization (Autorisation)

Authorization ist das Gewähren von Rechten, z. B. Zugriffsrechten im Datennetz.

B-Kanal

B-Kanal ist der Übertragungsweg für die Nutzdaten (Sprache, Daten) einer ISDN-Verbindung.

BLF Belegtlampenfeld

myPortal bietet ein sogenanntes Belegtlampenfeld BLF um den Gesprächszustand von hinterlegten Teilnehmern optisch anzuzeigen.

Broadcast

Ein Broadcast ist ein Rundruf in einem PC-Netzwerk. Dabei wird eine Nachricht (ein Datenpaket) von einem Punkt aus an alle Teilnehmer eines Netzes übertragen. Ein Broadcast wird in einem Datennetz verwendet, wenn die Adresse des Empfängers der Nachricht unbekannt ist.

CA (Certification Authority)

CA ist eine Organisation, die Zertifikate mit digitalen Signaturen ausstellt. Digitale Signaturen werden z. B. bei VPN (Virtual Private Network) benötigt.

CAPI-Schnittstelle (Common Application Programming Interface)

CAPI ist eine ISDN-konforme standardisierte Software-Schnittstelle.CAPI ermöglicht die Erstellung von ISDN-Software ohne Kenntnisse der herstellerspezifischen ISDN-Hardware.

Centrex

Centrex (Central Office Exchange) stellt Funktionen einer Telefonanlage via PSTN oder via ITSP bereit. Dies wird auch als virtuelle Telefonanlage, Hosted PBX (Private Branch Exchange) oder NetPBX bezeichnet.

CHAP (Challenge Handshake Authentication Protocol)

CHAP ist ein Authentifizierungsprotokoll, das im Rahmen des Point-to-Point-Protokolls eingesetzt wird.

COS (Class of Service)

QoS ist ein Verfahren, das die Übertragungsqualität von Daten in IP-Netzen gewährleistet.

CLIP (Calling Line Identification Presentation)

Durch die Rufnummernübermittlung wird die Rufnummer des Anrufers dem angerufenen Teilnehmer angezeigt. Der angerufene Teilnehmer kann dadurch vor der Gesprächsannahme den Anrufer identifizieren.

CLIR (Calling Line Identification Restriction)

Der Anrufer unterdrückt die Anzeige seine Rufnummer beim angerufenen Teilnehmer. Der angerufene Teilnehmer kann dadurch den Anrufer vor der Gesprächsannahme nicht identifizieren.

COLP (Connected Line Identification Presentation)

Mit Rufnummernübermittlung des Angerufenen wird dem Anrufer die Rufnummer des angerufenen Teilnehmers angezeigt, wenn die Verbindung zustandegekommen ist.

COLR (Connected Line Identification Restriction)

Mit Rufnummernunterdrückung des Angerufenen wird die Rufnummer vom angerufenen Teilnehmer beim Anrufer unterdrückt, obwohl der Anrufer COLP aktiviert hat.

Comfort User

Comfort User ist der Standart Benutzer des Kommunikationssystems.

Comfort Plus User

Der Comfort Plus User ist der Advanced User (Benutzer) des Kommunikationssystems im Gegensatz zum Comfort User kann der Comfort Plus User mehr Leistungsmerkmale (wie Fax, Mobility, Conferencing) nutzen.

CorNet

CorNet ist ein proprietäres Protokoll zur Vernetzung der HiPath- und OpenScape-Kommunikationssysteme. Im Gegensatz zum allgemein unterstützten QSIG sind in CorNet alle herstellerspezifischen Leistungsmerkmale der HiPath- und OpenScape-Kommunikationssysteme integriert.

CorNet-IP

CorNet-IP ist eine Protokollvariante von CorNet, welche eine Quervernetzung von Anlagen oder die Anbindung von Systemtelefonen (z. B. optiPoint) über IP ermöglicht.

CorNet-NQ

Ein proprietäres QSIG-basiertes Signalisierungsprotokoll für die Verbindung von Kommunikationssystemen mit einem oder mehreren QSIG-TK-Anlagen.

CSTA (PC Supported Telecommunications Applications)

CSTA ist eine Protokollschnittstelle für Anwendungen, die den European PC Manufacturers Association (ECMA)-Standard unterstützen. Über CSTA werden die Telekommunikationsaktivitäten über SIP gesteuert und überwacht.

CSV (Character Separated Values)

Eine CSV-Datei ist eine Textdatei zur Speicherung oder zum Austausch einfach strukturierter Daten. CSV steht dabei für Character Separated Values bzw. Comma Separated Values oder Colon Separated Values, weil die einzelnen Werte durch ein spezielles Trennzeichen, beispielsweise ein Komma oder ein Semikolon, getrennt werden. CSV-Dateien müssen im ANSI/ASCII-Format vorliegen.

CRL (Certificate Revocation Lists)

Eine CRL Zertifikatswiderrufliste ist eine Aufstellung sämtlicher widerrufener Zertifikate. CRLs müssen immer von der Zertifizierungsstelle erzeugt werden, von der die Zertifikate stammen.

Delay

Ein Delay hat in der Telekommunikation zwei Bedeutungen:

- Das Zeitintervall, um das ein Ereignis verzögert wird.
- Die Zeit zwischen dem Auftreten eines Ereignisses und dem Auftreten eines erwarteten Folgeereignisses.

Dedicated (dediziertes, fest zugeordnetes) Gateway

Wenn im LCR ein Dedicated Gateway für eine Richtung eingetragen ist, so wird zwingend über dieses Gateway geroutet. Anderslautende Regeln für das Routing sind dann ungültig.

DHCP (Dynamic Host Configuration Protocol)

DHCP ist ein Verfahren um einem PC beim Start bestimmte IP-Konfigurationen (IP-Adresse, Subnetzmaske, usw.) zugewiesen werden.

DS (DiffServ, Differentiated Services)

DS ist ein Verfahren zur Paketverwaltung in Datennetzen. Es wird angegeben, wie ein bestimmtes Datenpaket weitervermittelt werden soll und gibt einen bestimmten Service-Level in Bezug auf Bandbreite, Queueing-Theorie und Paketverwerfungs-Entscheidungen vor.

Diffie-Hellman-Algorithmus

Der Diffie-Hellman-Algorithmus dient dem Schlüsselaustausch bei VPN. Die aus diesem Algorithmus entstehenden Daten werden mit einem bestimmten Satz mathematischer Parameter konfiguriert. Damit der Schlüsselaustausch ordnungsgemäß funktioniert, müssen beide Teilnehmer identische Werte für diese Parameter verwenden.

DLI (Deployment License Service Integrated)

Über DLI kann man IP-Systemtelefone automatisch installieren und hochrüsten.

DMZ (Demilitarized Zone)

Eine DMZ (auch ent- oder demilitarisierte Zone) bezeichnet ein PC-Netzwerk mit sicherheitstechnisch kontrollierten Zugriffmöglichkeiten auf die daran angeschlossenen Netzwerkknoten (PC, Router, etc).

DNS (Domain Name Service)

Namensauflösung im Internet und auch im LAN. Namen von PCs oder Webseiten werden mittels DNS in die zugehörigen IP-Adressen umgesetzt.

DSL (Digital Subscriber Line)

DSL ist eine Technologie, um einen Internetzugang bereitzustellen, der über eine hohe Bandbreite verfügt. Mit der Technik DSL wird dabei die Strecke zwischen der Vermittlungsstelle des Providers und der Telefondose des Kunden überbrückt.

DSS (Direct Station Selection)

Die Funktionstasten eines Telefons oder Beistellgerätes können als Direktruftasten (DSS-Tasten) eingerichtet werden. Dafür werden diese mit der Rufnummer eines internen Teilnehmers oder einer Gruppe programmiert. Durch Drücken einer DSS-Taste wird ein sofortiger Anruf zum programmierten Ziel ausgeführt.

DTMF (Dual Tone Multifrequency)

Siehe MFV.

EIM (Enterprise Instant Messaging)

EIM ist ein Instant Messaging Dienst, der auf privaten Servern in einem Unternehmen auf Plattformen wie dem Live Communications Server oder Office Communications Server 2007 von Microsoft ausgeführt wird.

Enterasys-Switche

Enterasys-Switche werden von Enterasys Networks als sichere Netzwerklösungen produziert. Die stapelbaren Switche erkennen QoS-Features, klassifizieren und priorisieren Voice-, Video- und Daten-Applikationen.

ESP (Encapsulating Security Payload)

Bei ESP handelt es sich um ein IPSec-Protokoll, durch das die Paketverschlüsselung, Paketintegrität sowie die Paketauthentizität sichergestellt wird. Die Integritäts- sowie Authentizitätsprüfung erstreckt sich hierbei jedoch nicht auf den IP-Header sondern nur auf die eigentlichen Daten (Payload).

FoIP (Fax over IP)

FoIP ist eine Mehtode der Übermittlung von Faxnachrichten über ein IP-Netzwerk.

FTP

Das File Transfer Protocol (Dateiübertragungsverfahren) FTP ist ein im RFC 959 spezifiziertes Netzwerkprotokoll zur Dateiübertragung über TCP/IP-Netzwerke.

Funktionskennzahlen

Funktionskennzahlen sind Einwahlnummern bzw. Pilotnummern für z. B. Parken, Konferenz und AutoAttendant. Funktionskennzahlen entsprechen dabei virtuellen Teilnehmern. In einem Netzverbund müssen Funktionskennzahlen immer eindeutig sein.

G.711

G.711 ist ein Standard zur Digitalisierung von analogen Audiosignalen. Er wird in der klassischen Festnetz-Telefonie verwendet (PCM-Technik). Auch bei VoIP ist G.711 eine mögliche Sprachcodierung.

G.729AB

G.729 bezeichnet einen Codec zur Komprimierung von Sprache in digitale Signale und wird in der IP-Telephonie eingesetzt. G.729 ist sehr rechenaufwändig. Eine etwas vereinfachte, qualitativ aber geringfügig unterlegene Variante stellt G.729AB dar, die dafür weniger Rechenleistung benötigt.

Gateway / Gatewaymodule

Ein Gateway ist der Ein- bzw. Ausgang zu einem Kommunikationsnetz, es verbindet zwei verschiedene Datenverkehrsströme.

GSM (Global System for Mobile Communications

GSM ist ein Standard für digitale Mobilfunknetze, der hauptsächlich für Telefonie, aber auch für leitungs- und paketvermittelte Datenübertragung sowie Kurzmitteilungen (Short Messages) genutzt wird.

Handover

Als Handover bezeichnet man einen Vorgang in einem mobilen Kommunikationsnetz, bei dem das Mobiltelefon während eines Gesprächs oder einer Datenverbindung von einer Funkzelle in eine andere wechselt. Auch bei einem Wechsel zwischen GSM und UMTS mit einem Dual-Mode-Mobiltelefon spricht man von Handover.

Hash-Wert

Hash- bzw. Streuwerte sind meist skalare Werte aus einer Teilmenge der natürlichen Zahlen. Ein Hash-Wert wird auch als Fingerprint bezeichnet. Denn wie ein Fingerabdruck einen Menschen nahezu eindeutig identifiziert, ist ein Hash-Wert eine nahezu eindeutige Kennzeichnung einer Menge.

H.323

H.323 bezeichnet eine Gruppe von Standards, die eine Reihe von Medientypen für Paketnetze definieren. Die Standards decken Sprache, Daten, Fax und Video

ab und definieren, wie Signale von analog in digital umgewandelt werden und welche Signalisierung verwendet werden soll.

OpenScape Business Assistant

OpenScape Business Assistant dient der Administration des Kommunikationssystems. Hier finden sie alle Wizards zur schnellen Unterstützung von Administrationsaufgaben.

Hosted Services

Hosted Services oder Gehostete Dienste sind traditionelle IT-Dienste wie E-Mail, Instant Messaging IM und Unified Communications UC, die ein Internet Provider einem Unternehmen von einem Remote-Standort aus bereitstellt; sodass für das Unternehmen die Notwendigkeit entfällt, diese Dienste auf eigenen Servern vor Ort zu verwalten und auszuführen.

ICMP (Internet Control Message Protocol)

ICMP dient in Datennetzen zum Austausch von Informations- und Fehlermeldungen über das Internet-Protokoll IP.

IDS (Intrusion Detection System)

IDS ist ein Sicherheitssystem, das alle ein- und ausgehenden Netzwerkaktivitäten überwacht, um mögliche Sicherheitsverletzungen zu identifizieren. Hierzu gehört sowohl das Eindringen (Angriffe von außerhalb der Organisation) als auch der Missbrauch (Angriffe von innerhalb der Organisation).

IEEE-Standards

IEEE-Standards sind ein Satz von Spezifikationen, die vom Institute of Electrical and Electronic Engineers (IEEE) definiert wurden (zum Beispiel Token Ring, Ethernet), um gemeinsame Netzwerkstandards für Hersteller einzurichten.

IEEE 802.1p

IEEE 802.1p ist ein Standard der IEEE, der den Transport von Datenpaketen unterschiedlicher Priorität in Rechnernetzen regelt. Die Datenpakete werden in Prioritätsklassen von 1 bis 7 eingeteilt. Der Standard legt nur fest das die Priorität von 1 bis 7 steigt, trifft aber keine weitergehenden Aussagen darüber wie die Datenpakete im einzelnen behandelt werden sollen.

IKE-Protokoll

Das IKE -Protokoll hat zwei verschiedene Aufgaben. Zunächst ist eine ausschließlich vom IKE-Protokoll genutzte SA (Security Association) herzustellen (IKE-SA). Anschließend wird die vorhandene IKE-SA zur sicheren Aushandlung aller weiteren für die Übertragung von Payload-Daten benötigten SAs (Payload-SA) genutzt.

IM (Instant Messaging)

IM ist ein Verfahren zum Echtzeitaustausch von Textnachrichten über das Internet mithilfe von PCs, Pocket-PCs und Mobiletelefonen. Moderne IM-Dienste

ermöglichen VoIP und Videokonferenzen, Dateitransfer und Desktop-Application-Sharing.

IP PBX

IP PBX ist eine Kommunikationsanlage, die sowohl VoIP-Verbindungen als auch Sprachverbindungen über herkömmliche Telefonleitungen unterstützt.

IPSec

IPSec ist ein Gerüst offener Standards für die Gewährleistung vertraulicher, sicherer Kommunikationsverbindungen über IP-Netzwerke durch Einsatz verschiedener Sicherheitsdienste und -protokolle.

ISP (Internet-Service-Provider)

Ein ISP ist ein Unternehmen, das Einzelpersonen, Firmen und anderen Organisationen Dienste zur Anbindung an das Internet anbietet. Einige ISPs sind große nationale oder internationale Unternehmen, die den Zugang an einer Vielzahl von Standorten anbieten, während andere ISPs auf einzelne Orte oder Regionen beschränkt sind.

ITSP (Internet-Telefonie-Service-Provider)

Ein ITSP ist ein Unternehmen, das Einzelpersonen, Firmen und anderen Organisationen Telefondienste über das Internet anbietet.

IWV (Impulswahlverfahren)

IWV ist das älteste Signalisierungsverfahren der automatischen Telefonvermittlung. IWV ist heute meistens von MFV abgelöst.

Jitter

Unter Jitter versteht man eine Verzögerung von Datenpaketen bei Sprachübertragungen. Eine zu große Verzögerung zwischen dem Senden von Datenpaketen und ihrem Eingang am empfangenden Ende macht die Sprachkommunikation unregelmäßig und schwer verständlich.

KWI (Kurzwahl individuell)

Mit Hilfe der Kurzwahl individuell KWI können zusätzlich zur Kurzwahl zentral von jedem dazu berechtigtem Telefon 10 externe individuelle Kurzwahlnummern gespeichert werden.

KWZ (Kurzwahl zentral)

Häufig benötigte externe Telefonnummern können im Systemspeicher des Kommunikationssystems hinterlegt werden. Jede Nummer wird durch eine Kurzwahlnummer vertreten, die anstelle der vollständigen Telefonnummer von allen Teilnehmern genutzt werden kann.

Latenz

Unter Latenz versteht man die Zeit, die für den Transport eines Datenpakets von einer Anwendung zur anderen benötigt wird, einschließlich der Zeitdauer für die

Übermittlung über das Netzwerk und für die Vorbereitung und Verarbeitung der Daten am sendenden und am empfangenden Gerät.

LCR (Least Cost Routing)

Mit Hilfe von LCR (Least Cost Routing, Leitwenkung) legen Sie fest, über welchen Anbieter z. B. Amts, Handy- oder Auslandsgespräche geführt werden. Sie legen über das Kommunikationssystem den kostengünstigsten Anbieter fest und führen alle entsprechenden Gespräche über diesen definierten Weg.

LIN (Location Identification Number)

LIN ist eine eindeutige max. 16stellige Nummer, die dem 10-stelligen NANP (North American Numbering Plan) entspricht.

LWCA (Leightweight CA)

LWCA ist eine eingeschränkte Zertifizierungsfunktion.

Media Stream Channel

Ein Media Gateway kann leitungsvermittelte B-Kanäle des ISDN terminieren und aus der darin übertragenen Sprachinformation Media Stream Channels für ein IP-basiertes Paket-Netzwerk erzeugen. Media Stream Channels enthalten eine Kombination von Audio-, Video-, und T.120-Medien.

MFV (Mehrfrequenzwahlverfahren)

Das Mehrfrequenzwahlverfahren MFV (auch Tonwahlverfahren) ist das Wahlverfahren in der analogen Telefontechnik und das heute überwiegend in der Vermittlungstechnik genutzte Verfahren zur Übermittlung der Rufnummer an das Telefonnetz.

MIM (Mobile Instant Messaging)

MIM ist ein Presence- und Instant-Messaging-Dienst für mobile Telefone.

Mobility

Mobility bezeichnet die Nutzung von Pocket-PCs und mobilen Telefonen und deren Integration in das Kommunikationssystem einer Firma.

MOH (Music on Hold)

Anrufern kann Wartemusik (MOH, Music on Hold) eingespielt werden, wenn diese nicht sofort vermittelt werden können.

MSN (Multiple Subscriber Number)

Beim Anschluss von ISDN-Telefonen über einen S0-Bus (Mehrgeräteanschluss) wird jedem einzelnen ISDN-Telefon (ISDN-Teilnehmer) eine eindeutige Multiple Subscriber Number MSN zugeordnet. Die ISDN-Teilnehmer sind über ihre MSN erreichbar.

MULAP (Multiple Line Appearance)

MULAPs sind spezielle Gruppen in denen mehrere Telefone zusammengefasst sind. Einem Gruppenmitglied können dabei unter einer Rufnummer mehrere Telefone zugeordnet werden (Basic-MULAP). Ausserdem können in einer solchen Gruppe spezielle Leistungsmerkmale, die für die Kommunikation zwischen Chef und Sekretär bzw. in Teams erforderlich sind, realisiert werden (Chef-MULAP, Team-MULAP).

Multi-Gateway

Bei einer Multi-Gateway-Vernetzung werden die Anrufe über mehrere, verschiedene Gateways geroutet.

myAttendant

myAttendant ist der Vermittlungsplatz des Kommunikationssystems.

myPortal

myPortal ist das Java-basierte Benutzerportal für den Zugriff der Teilnehmer auf die Unified Communications Funktionen. Neben Informationen über den Anwesenheitsstatus, komfortablen Wahlhilfen über Favoriten und Verzeichnisse, hat der Teilnehmer auch Zugriff auf Sprachnachrichten und Faxe.

myPortal for Outlook

myPortal for Outlook ist das in Microsoft Outlook integrierte Benutzerportal für den Zugriff der Teilnehmer auf die Unified Communication Funktionen, analog zu myPortal. Zusätzlich bietet myPortal for Outlook eine komfortable Desktop-Wahl.

NAC (Network Admission Control)

NAC ist eine Technologie, die die Abwehr von Viren und Würmern aus dem Netzwerk heraus unterstützt. Mit NAC werden Endgeräte während der Authentisierung auf Richtlinienkonformität geprüft. Ist z. B. der Virenscanner nicht aktuell oder fehlt dem Client-Betriebssystem der neueste Security-Patch, wird das betroffene Endgerät unter Quarantäne gestellt und mit aktuellen Updates versorgt bis es wieder den geltenden Sicherheitsrichtlinien entspricht.

NAT (Network Address Translation)

NAT ist ein Verfahren, um eine IP-Adresse in einem Datenpaket durch eine andere zu ersetzen. Dies wird genutzt, um private IP-Adressen auf öffentliche IP-Adressen abzubilden. Werden auch die Port-Nummern umgeschrieben, spricht man dabei von Maskieren oder PAT (Port Address Translation).

NTBA (Network Termination for ISDN Basic Access)

Ein NTBA (Network Termination for ISDN Basic Acces), oder auch NT (Network Termination) genannt, ist das Netzabschlussgerät für den ISDN-Basisanschluss. Er ist das Bindeglied zwischen dem digitalen Netz des Netzbetreibers und den ISDN-Einrichtungen auf der Teilnehmerseite.

NTPM (Network Termination for Primary Rate Multiplex Access)

Ein NTPM (Network Termination for Primary Rate Multiplex Access) ist das Netzabschlussgerät für den ISDN-Primärmultiplexanschluss. Er ist das Bindeglied zwischen dem digitalen Netz des Netzbetreibers und den ISDN-Einrichtungen auf der Teilnehmerseite.

OLSR

OLSR ist ein spezielles Ad-hoc-Protokoll, mit dem es ermöglicht wird, die auf OSI-Schicht 2 fehlende Möglichkeit des Routing auf OSI-Schicht 3 nachzurüsten.

ONS (One Number Service)

Rufnummer, die einem Benutzer direkt zugeordnet ist. Einem Benutzer können mehrere Ressourcen (Telefone) zugeordnet werden. Wird er über die ONS-Nummer angerufen, wird der Anruf an das Telefon weitergeleitet, das der Benutzer aktuell nutzt (z. B. das Mobiltelefon).

PAP (Password Authentication Protocol)

PAP ist ein Verfahren zur Authentifizierung über das Point-to-Point-Protocol. Es wird für die Einwahl zu einem ISP verwendet. Bei PAP wird das Passwort für die Authentifizierung im Klartext zusammen mit einer User-ID übertragen.

PBX (Private Branch Exchange)

Eine PBX (Telefonanlage) ist eine Vermittlungseinrichtung, die mehrere Endgeräte wie zum Beispiel Telefon, Fax, Anrufbeantworter sowohl untereinander als auch mit dem öffentlichen Telefonnetz verbindet.

Peer

Als Peer wird der Endpunkt einer Kommunikation in einem Peer-to-Peer-Netzwerk bezeichnet. Jeder Peer bietet dabei seine Dienste an und nutzt die Dienste der anderen Peers.

Peer-to-Peer

In einem Peer-to-Peer-Netz sind alle PCs gleichberechtigt und können sowohl Dienste in Anspruch nehmen als auch Dienste zur Verfügung stellen.

Peer-Instanz-Authentifizierung

Die Authentifizierung der Peer-Instanz in einer Verbindung stellt sicher, dass diese den Angaben entspricht.

PKI (Public Key Infrastructure)

Mit PKI bezeichnet man in der Kryptologie und Kryptografie ein System, welches es ermöglicht, digitale Zertifikate auszustellen, zu verteilen und zu prüfen. Die innerhalb einer PKI ausgestellten Zertifikate werden zur Absicherung computergestützter Kommunikation verwendet.

PPP (Point-to-Point-Protokoll)

PPP ist ein IETF-Standard zur Übertragung von IP-Paketen über serielle Leitungen. PPP wird vor allem für die Einwahl ins Internet genutzt.

PPPoE (Point-to-Point-Protokoll over Ethernet)

Das PPPoE-Protokol (PPP over Ethernet) ist die Verwendung des Netzwerkprotokolls Point-to-Point über eine Ethernet-Verbindung.

Pre-shared Key

Der Pre-shared Key ist ein Schlüssel, der bei der Tunnelkonfiguration (bei VPN) festgelegt wird. Damit sich die über den Tunnel kommunizierenden VPN-Partner, authentifizieren können, muss für beide Tunnelendpunkte das gleiche Kennwort verwendet werden.

PPTP (Point-to-Point-Tunneling-Protokoll)

PPTP ist eine Technologie, mit der ein Virtuelles Privates Netzwerk (VPN) eingerichtet werden kann. Da das Internet im Grunde ein offenes Netzwerk ist, wird mithilfe von PPTP sichergestellt, dass Nachrichten, die von einem VPN-Knoten zu einem anderen übertragen werden, sicher sind. Mit PPTP können sich Benutzer über das Internet in ihr Firmennetz einwählen.

Präsenz (Presence)

Der Begriff Präsenz oder Anwesenheit steht für die Fähigkeit eines Unified Communication Systems, jederzeit feststellen zu können, wo sich ein Benutzer befindet und welchen Status er hat. Dadurch kann bei der Kommunikation mit diesem Teilnehmer per Telefon, E-Mail, Instant Messaging oder Fax besser auf dessen Wünsche eingegangen werden.

Proxy-Server

Der Proxy-Server ist das Verbindungsglied zwischen Client-Applikation und Web-Server. Seine Aufgabe ist es, die Anforderungen der Client-Applikation zu filtern und den Web-Server zu entlasten.

PSTN (Public Switched Telephone Network)

PSTN bezeichnet das öffentliche, leitungsgebundene Telefonnetz. Öffentliche Netze können in staatlichem oder privatem Besitz sein.

QOS (Quality of Service)

Für Voice over IP ist es wichtig, eine Mindestbandbreite für die Dauer der Übertragung sicherzustellen. Wenn mehrere Applikationen gleichberechtigt über IP arbeiten, so wird die vorhandene Bandbreite einer Übertragungsstrecke aufgeteilt, so dass unter Umständen eine Sprachverbindung von Paketverlusten betroffen ist, woraus eine schlechte Sprachqualität resultieren kann. Es gibt unterschiedliche Verfahren um die höchstmöglich Qualität bei der Übertragung zu gewährleisten, bei diesen Verfahren spricht man von Quality of Service (QOS).

RAS (Remote Access Service)

Ein RAS- (Remote Access Service) User ist ein IP-Teilnehmer (z. B. ein Teleworker), der sich per Remote am System anmeldet und sich wie ein interner IP-Teilnehmer verhält. Er kann somit den kompletten Leistungsumfang des Kommunikationssystems nutzen.

RJ45 (Registered Jack 45)

RJ45 ist eine achtpolige Steckverbindung, die z. B. für die Verbindung von 10BaseT-Kabel in der Netzwerktechnik eingesetzt wird.

Roaming

Roaming ist die Fähigkeit eines Mobilfunknetz-Teilnehmers, in einem fremden Netzwerk als seinem Heimnetzwerk automatisch zu telefonieren oder Zugriff auf andere Mobilfunknetzdienstleistungen zu haben.

RTCP (Real-Time Control Protocol)

Das RealTime Control Protocol (RTCP) dient der Aushandlung und Einhaltung von Quality of Service (QoS) Parametern durch den periodischen Austausch von Steuernachrichten zwischen Sender und Empfänger.

RTP (Real-Time Transport Protocol)

RTP ist ein IETF-Standard für das Streaming von Echtzeit-Multimediadaten über das Internet-Protokoll. RTP setzt normalerweise auf das UDP-Protokoll auf und verwendet dynamische UDP-Ports, die zwischen dem Sender und dem Empfänger spezieller Medienstreams ausgehandelt werden.

RTT (Round Trip Time)

RTT ist das Zeitintervall, das ein Datenpaket benötigt, um von der Quelle zum Ziel und zurück zu gelangen.

SA (Security Association)

SA ist eine Sicherheitsverbindung zwischen zwei kommunizierenden Einheiten in Rechnernetzen. Sie beschreibt, wie die beiden Parteien Sicherheitsdienste anwenden, um miteinander kommunizieren zu können.

SDSL (Symmetric Digital Subscriber Line)

SDSL eignet sich besonders für Internet-Telefonie, Intranet-Anwendungen in Firmen bei Standortvernetzungen, für Videokonferenzen und ist z. B. prädestiniert für Teleworker, die dadurch Daten mit der gleichen Bandbreite senden und empfangen können. Im Gegensatz zu ADSL sind die Bandbreiten bei SDSL vom und zum Internet gleich hoch.

Secure CLI

Secure CLI ist ein Sicherheitsmerkmal, das mithilfe von SFTP (Secure File Transfer Protocol) sichere Befehlszeilen- und Dateiübertragungs-Schnittstellen bereitstellt.

SFTP (Secure File Transfer Protocol)

SFTP ist ein Sicherheitsprotokoll zur Übermittlung von Verbindungsdatensätzen.

ShrewSoft VPN-Client

Der ShrewSoft VPN-Client ist ein quelloffener und kostenloser VPN-Client mit grafischer Oberfläche. Er beinhaltet unter anderem ISAKMP, Xauth- und RSA-Unterstützung, AES, Blowfish, 3DES-Verschlüsselungsprotokolle.

Single-Gateway

Bei einer Single-Gateway-Vernetzung werden die Anrufe über ein einziges Gateway geroutet.

SIP (Session Initiation Protokoll)

SIP ist ein im RFC 3261 spezifiziertes Internet-Standardprotokoll zum Aufbau und Steuerung von Sprachverbindungen und Videokonferenzen über ein IP-Netzwerk.

SNMP (Simple Network Management Protocol)

SNMP ist ein Verfahren um Informationen über den Zustand von Netzwerkkomponenten und PCs zu bekommen.

SPE (Signaling and Payload Encryption)

Signaling & Payload Encryption (SPE) dient der Sicherheit der Übertragung von Sprachdaten. Es werden VoIP-Nutz- und Signalisierungsdatenströme vom und zum Gateway und zwischen IP-Telefonen verschlüsselt.

SRTP (Secure Real-Time Transport Protokoll)

SRTP ist ein verschlüsseltes RTP-Protokoll. Es eignet sich besonders zur Übertragung von Kommunikationsdaten über das Internet, und findet in der IP-Telefonie Verwendung.

SSH (Secure Shell)

SSH ist ein Protokoll, das Unterstützung für sichere Remote-Anmeldung, sicheren Dateitransfer und sichere TCP/IP-Umleitungen bietet. Es kann übertragene Daten automatisch verschlüsseln, authentifizieren und komprimieren.

SSL (Secure Socket Layer)

SSL ist ein Protokoll für die Übertragung von Dokumenten über das Internet. Bei SSL werden Daten mit einem privaten Schlüssel versehen, bevor sie übertragen werden. URLs, die eine SSL-Verbindung erfordern, beginnen immer mit https: statt mit http:.

Status

Der Status gibt (im Zusammenhang mit dem Begriff "Präsenz") an, ob ein Teilnehmer verfügbar, besetzt, offline etc. ist, sodass andere Teilnehmer im Kommunikationssystem wissen, ob dieser Teilnehmer erreichbar ist.

STUN (Simple Traversal of UDP over NAT)

STUN ist ein Netzwerkprotokoll um das Vorhandensein und die Art von Firewalls und NAT-Routern zu erkennen und diese zu umgehen.

Survivability

Survivability ist die Fähigkeit eines Netzverbundes, den Service auch bei vorhandenen Fehlern im Netzwerk aufrechtzuerhalten.

TAE (Telekommunikations-Anschluss-Einheit)

TAE ist eine Steckerart bei analogen Telefonanschlüssen mit a/b-Schnittstelle und bei ISDN-Anschlüssen zum Anstecken des NTBA an die Anschlussleitung. Anschließbar sind analoge Telefone, Faxgeräte und ISDN-Telefonanlagen.

TCP (Transmission Control Protocol)

TCP ist ein Protokoll das regelt, auf welche Art und Weise Daten zwischen PCs ausgetauscht werden sollen. Alle Betriebssysteme moderner PCs beherrschen TCP und nutzen es für den Datenaustausch mit anderen PC.

TFTP (Trivial File Transfer Protocol)

TFTP ist ein Datenübertragungsprotokoll und unterstützt das Lesen und Schreiben von Dateien. Viele Funktionen des übergeordneten FTP-Protokolls sind bei TFTP nicht vorhanden, z. B. Rechtevergabe, Anzeigen der vorhandenen Dateien oder Benutzerauthentifizierung.

Telnet

Ein Protokoll, das zwei PCs miteinander verbindet, um eine Terminalverbindung zum entfernten PC bereitzustellen. Der Benutzer wählt sich nicht in den PC ein, sondern stellt die Verbindung über das Internet per Telnet her. Der Benutzer initiiert eine Telnet-Sitzung, stellt die Verbindung zum Telnet-Host her und meldet sich an. Über die Verbindung kann der Benutzer mit dem entfernten PC arbeiten, und sein eigenes System erscheint auf dem fernen PC wie ein lokal angeschlossenes Terminal.

TOS (Type of Service)

TOS ist ein Feld im Header von IP-Datenpaketen und wird für die Priorisierung dieser Pakete gesetzt und ausgewertet (z. B. bei Quality of Service).

UCD (Uniform Call Distribution)

UCD ermöglicht eine geichmäßige Verteilung von eingehenden Anrufen im Kommunikationssystem auf eine Gruppe von Teilnehmern (UCD-Gruppe).

UDP (User Datagram Protocol)

UDP ist ein Netzprotokoll, das zur Transportschicht der Internetprotokollfamilie gehört. UDP übergibt Daten, die über das Internet übertragen werden, an die jeweilige Anwendung.

UMTS (Universal Mobile Telecommunications System)

UMTS ist ein Mobilfunkstandard der dritten Generation mit dem deutlich höhere Datenübertragungsraten (384 kbit/s bis 7,2 Mbit/s), als mit dem Mobilfunkstandard der zweiten Generation oder dem GSM-Standard, möglich sind.

Unified Communications

Unified Communications ist die Integration unterschiedlicher Kommunikationssysteme, -medien, -geräte und –anwendungen innerhalb einer Umgebung (z. B. IP-Telefonie, ortsgebundene und mobile Telefonie, E-Mail, Instant Messaging, Desktop-Anwendungen, Sprachbox, Fax, Konferenzen und Unified Messaging).

Unified Messaging

Unified Messaging ist die Integration unterschiedlicher Kommunikationsdaten wie E-Mail, SMS, Fax, Telefonie etc. in einen einheitlichen Nachrichtenspeicher. Dieser Nachrichtenspeicher ist über eine Vielzahl unterschiedlicher Geräte erreichbar.

VAD (Voice Activity Detection)

VAD (Voice Activity Detection) bezeichnet eine automatische Sprechpausenerkennung bei der digitalen Übertragung von Audiodaten.

VCAPI-Schnittstelle

VCAPI ist eine virtuelle CAPI-Schnittstelle, die das Vorhandensein einer lokalen ISDN-Karte emuliert. Ist im internen Netz eine ISDN-Karte in einem PC eingebaut, so kann allen Teilnehmern im Netz diese ISDN-Karte über die VCAPI-Schnittstelle zur Verfügung gestellt werden.

VDSL (Very High Speed Digital Subscriber Line)

VDSL kommt überall dort zum Einsatz, wo über kurze Entfernungen symmetrische oder asymmetrische Datenströme mit hoher Geschwindigkeit zu übertragen sind. VDSL stellt eine Alternative zu ADSL und SDSL dar und bietet zusätzlich höhere Übertragungsgeschwindigkeiten.

VoIP (Voice over IP)

VoIP ist die Übertragung von Sprachdaten über IP-basierte Netzwerke.

VPN (Virtual Private Network)

VPN nutzt die öffentliche Infrastruktur des Internets für Standortvernetzungen und Zugänge für Teleworker. Durch Verschlüsselungs- und Authentifizierungsmechanismen wird erreicht, dass externe Partner eine sichere Verbindung zum internen Datennetz erhalten.

WAN (Wide Area Network)

WAN ist die Bezeichnung für Weitverkehrsdatennetze, z. B. das Internet.

WBM (Web-Based-Management)

WBM ist eine Bedienoberfläche, die mittels HTML- oder JAVA-Seiten und einem Web-Protokoll, in einem Internet-Browser angezeigt wird.

X.509-Standard (VPN-Zertifikat)

X.509 ist ein ITU-T-Standard für eine Public-Key-Infrastruktur und derzeit der wichtigste Standard für digitale Zertifikate.

XMPP (Extensible Messaging and Presence Protocol)

Internetstandard der primär für Instant Messaging eingesetzt wird. XMPP unterstützt die Interaktion mit Benutzern anderer Netzwerke wie z. B. AIM, ICQ oder Windows Live Messenger (WLM). XMPP und seine Erweiterungen unterstützen unter anderem Konferenzen mit mehreren Benutzern (z. B. Multi-User Chat) und das Anzeigen des Online-Status.

Zweitgradig

Zweitgradig bedeutet, dass ein Teilnehmer telefoniert und zusätzlich steht bei diesem Teilnehmer bereits ein zweiter Ruf an.

Stichwörter

A

Ablauf der Lizenzierung 284
Abteilungen 514
Abteilungen, Experten-Modus 1595
Abwesenheitstexte 600
Abwurf/VPL/Hotline, Experten-Modus 1445
Ad-hoc-Konferenz 529
Ad-hoc-Konferenz (UC Smart) 464
Admin.-Protokoll-Daten, Experten-Modus 1425
Admin-Protokoll 980
  Admin.-Protokoll-Daten, Experten-Modus 1425
  Konfiguration, Experten-Modus 1425
  laden 980
  Sprache ändern 933, 934, 935, 980
Admin-Protokoll, Experten-Modus 1425
AF/EF-Codepunkte 399
Aktionen
  Automatische Aktionen, Experten-Modus 1427, 1428
  Manuelle Aktionen, Experten-Modus 1426
Aktionen, Experten-Modus 1426
Aktive Dienste, Experten-Modus 1472
Aktive Regeln, Experten-Modus 1479
Aktive Tunnel, Experten-Modus 1473
Aktive Zertifikate, Experten-Modus 1469
Aktivierung, Software (siehe Software-Aktivierung)
Aktualisierung, Software (siehe Software-Aktualisierung)
Aktualisierungszeit der DNS Namen, Experten-Modus 1453
Alarm-Signalisierungs, Experten-Modus 1421
Alle Leases, Experten-Modus 1496
alternativer Arbeitsplatz 502
Amtsberechtigung 685
  Erlaubnisliste anzeigen 691
  Filter für Verbotsliste ändern 691
  konfigurieren 689, 693, 694
  Rufnummer zur Erlaubnisliste hinzufügen 690
  Rufnummer zur Verbotsliste hinzufügen 690
  Verbotsliste anzeigen 691
Amtszugang
  ISDN-Amtszugang konfigurieren 371
Analoges Telefon 411
Analoge Teilnehmer, Experten-Modus 1524
Anklopfen/Rufeinblendung 596
Anruf
  entgangen 516
  geplant 516
Anrufbeantworter 411
Anrufbeantworter-Gruppe (siehe Sprachbox-Gruppe)
Anrufe abweisen 593
Anrufschutz 594
Anrufübernahme, Experten-Modus 1555
Anrufübernahmegruppe 610
  Anrufübernahme außerhalb einer AUN-Gruppe 611
  Anrufübernahme von Wiederanrufen 610
  Anrufübernahme von Wiederanrufen aktivieren 629, 999
  Anrufübernahme von Wiederanrufen deaktivieren 630, 999
  Aufmerksamkeitston 610
  Aufmerksamkeitston aktivieren 629
  Aufmerksamkeitston deaktivieren 629
  konfigurieren 619
  Mitglied hinzufügen 620
  Mitglied löschen 620
  Namensanzeige des Anrufers 610
  Namensanzeige des Anrufers aktivieren 628
  Namensanzeige des Anrufers deaktivieren 628
  Rufnummernanzeige des Anrufers 610
  Rufnummernanzeige des Anrufers aktivieren 628
  Rufnummernanzeige des Anrufers deaktivieren 628
  SIP-Telefone 610
Anrufumleitung 588
  regelbasiert 503
  statusbezogen 503
Anrufverteilung 670, 671
  AICC (Automatic Incoming Call Connection) 677
  Ansagen 682
  Ansagen ändern 682
  Konfiguration 670
  konfigurieren 672
  Nachbearbeitungszeit 675
  Nachbearbeitungszeit ändern 676
  Nachtschaltung 681
  Priorität externer Anrufe 676
  Priorität externer Anrufe ändern 677
  Priorität interner Anrufe 676
  Priorität interner Anrufe ändern 677
  Teilnehmerzustand 673
  Übergabe an UCD-Gruppe 683

Übergabe an UCD-Gruppe, Wiederanrufzeit ändern 683
Überlauf 680
Überlauf ändern 680
UCD-Agent 673
UCD-Agent hinzufügen 674
UCD-Agent löschen 675
UCD-Anrufe automatisch annehmen 677
UCD-Anrufe automatisch annehmen, aktivieren 678
UCD-Anrufe automatisch annehmen, deaktivieren 678
UCD-Anrufe über analoge Leitungen auslösen 684
UCD-Anrufe über analoge Leitungen auslösen, Auslösezeit ändern 684
UCD-Gruppe 671
UCD-Gruppe konfigurieren 672
Wartemusik (Music On Hold MOH) 682
Wartemusik (Music On Hold MOH) ändern 682
Warteschlange 678
Warteschlange ändern 679
Ansagen bei Anrufverteilung 682
Ansagen für Sprachbox 537
Ansagen und Wartemusik, Experten-Modus 1578
Anschaltungen
Ansage/Interne Wartemusik, Experten-Modus 1578
SmartVM, Experten-Modus 1579
Türsprechstelle, Experten-Modus 1579
Anschaltungen, Experten-Modus 1544, 1578
Anschlussbereich
OpenScape Business S 59
OpenScape Business UC Booster Server 59
Anwesenheitsstatus
Anrufumleitung 503
Anwesenheitsstatus (UC Smart) 459
Anwesenheitsstatus (UC Suite) 499
Application Firewall, Experten-Modus 1462
Application Launcher 1159, 1618
Profil für Konfigurationsdaten 1160
Application Launcher, Experten-Modus 1617
Applikat.-Diagnose
Entwickler-Einstellungen, Experten-Modus 1429
Mainboard, Experten-Modus 1429
Applikat.-Diagnose, Experten-Modus 1428
Applikationen, Experten-Modus 1591, 1618
Applikationsauswahl 1591
Applikationsgesteuerte Konferenz 523
Applikation-Suite, Experten-Modus 1539
ARP-Protokoll, Experten-Modus 1429
Audio-Codec 395
Parameter einem Ziel zuordnen 397
Parameter konfigurieren 396
Audio-Datei 1191, 1193
Aufschalten 598
Aufzeichnen 520
Ausbaugrenzen 1374
Ausnahme
regelbasierte Anrufumleitung 503
AutoAttendant 558
Automatische Aktion 1242
DLS Notification 1244
DLS Notification ändern 1245
DLS Notification starten 1246
DLS Notification stoppen 1246
Garbage Collection 1242
Garbage Collection ändern 1242
Garbage Collection starten 1244
Garbage Collection stoppen 1244
Automatische Nachtschaltung, Experten-Modus 1577
Automatischer Rückruf 596
Automatische Updates 489

B

Backup (siehe Sichern)
Backup-Medium 1201, 1204
bearbeiten 1206
hinzufügen 1205
löschen 1206
Backup-Set 1201, 1202, 1203
anzeigen 1203
sichern, sofort 1207
sichern, zeitgesteuert 1209
wiederherstellen 1210
Backup-Set für Diagnosezwecke 1291
erzeugen 1292
Backup-sofort 1207
Backup-Verzeichnis 1202
Bandbreiten im LAN 994
Bandbreiten im WAN 995
Basestations, Experten-Modus 1526
Basic-MULAP 651
ändern 657
anzeigen 657
hinzufügen 656
löschen 658
Mitglied ändern 659
Mitglied hinzufügen 658
Mitglied löschen 658
Rufart 652
SIP-Telefone 653
Basisstationen, Experten-Modus 1403, 1548
Baugruppen
nicht unterstützt 1367

Baugruppen-Zustand, Experten-Modus 1405
Bedingung
regelbasierte Anrufumleitung 503
Benachrichtigung
Faxnachricht 551
Sprachnachricht 474, 551
Benachrichtigungsdienst 474, 551
Benutzer-Profile der UC Suite 495
Benutzerschaltflächen 801
Layout 801
Benutzerverzeichnis, Experten-Modus 1594
Benutzer von UC Smart
Daten ändern 458, 474
Benutzer von UC Suite 489
als Agent konfigurieren 492
Anwesenheitsstatus ändern 493
Daten ändern 491
Kennwort ändern 494
Kennwortlänge ändern 494
zurücksetzen 492
Berechtigungen
Automatische Nachtschaltung, Experten-Modus 1577
Erlaubnislisten, Experten-Modus 1574
Nacht
Berechtigungsgruppen, Experten-Modus 1573
Nachtschaltung, Experten-Modus 1575
Sondertage, Experten-Modus 1578
Tag
Berechtigungsgruppen, Experten-Modus 1573
Teilnehmer, Experten-Modus 1572
VBZ Gruppenzuordnung, Experten-Modus 1576
VBZ Matrix, Experten-Modus 1576
Verbotslisten, Experten-Modus 1575
Berechtigungen, Experten-Modus 1572
Bestimmungsgemäßer Gebrauch der Kommunikationssysteme und Server 57
Betriebsbedingungen (klimatisch, mechanisch)
OpenScape Business X3, X5, X8 64
OpenScape Business S 64
OpenScape Business UC Booster Server 64
Blitzschutzanforderungen 60
Blockwahl 560
Branding, Experten-Modus 1398
Brandschutzanforderungen 60
Breitbandverbindung 331

C

CallMe 502
CallMe-Dienst 502
Call Monitoring, Experten-Modus 1412
Carrier Select Override 705
CDP Certificate Distribution Point 973
CE-Kennzeichnung 61
CE-Konformität 62
Central License Server (siehe Lizenzserver)
Chef/Sekretär (siehe Chef/Sekretär-Konfiguration)
Chef/Sekretär-Konfiguration 636
ändern 644
Eigenschaften eines Mitglieds ändern 650
Faxbox 639
Faxbox hinzufügen 650
hinzufügen 643
löschen 645
Mitglied ändern 650
Mitglied hinzufügen 649
Mitglied löschen 649
Rufart 639
SIP-Telefone 639
Chef-Funktion (siehe Chef/Sekretär-Konfiguration)
Chef-MULAP 653
ändern 660
anzeigen 660
hinzufügen 659
löschen 660
Mitglied ändern 661
Mitglied hinzufügen 661
Mitglied löschen 661
Rufart 655
SIP-Telefone 655
CLA
lokale Verbindung 294, 295, 307
zentrale Verbindung 307
Classes Of Service, Experten-Modus 1507
Client (UC Smart) 454
Client (UC Suite) 477
Client Logs 1298
herunterladen 1302
Clients, Hard- und Softwarevoraussetzungen 482, 781, 812, 816
Clipboard-Wahl 519
CLIP no screening 576
CLIP - Rufnummernübermittlung des Anrufers 572
CLIR - Rufnummernunterdrückung des Anrufers 574
CMD (CSTA Message Dispatcher) 1619
Codec-Parameter, Experten-Modus 1512
Codeschloss individuell 701
COLP - Rufnummernübermittlung des Angerufenen 575
COLR - Rufnummernunterdrückung des Angerufenen 575
Communities, Experten-Modus 1423
Contact Center 809
Agent 819

Agent aus einer Warteschlange entfernen 880
Agent einer Warteschlange zuordnen 879
Agentenrückruf 831
Ansage aufnehmen 855
Ansage laden 856
Anzeige der Warteschlangendetails 831
Bedingungen für den Betrieb 881
Beispiel für eine Contact-Center-Konfiguration 836
Berechtigungs-Level eines Agenten 819
Berichte 885
Berichts-Designer 886
bevorzugte Agenten 821
bevorzugten Agenten festlegen 873
bevorzugten Agenten löschen 873
CCV-Objekte 768, 824
Clients 810
einfache Nachbearbeitung, Nachbearbeitungsgrund ändern 876
einfache Nachbearbeitung, Nachbearbeitungsgrund hinzufügen 875
einfache Nachbearbeitung, Nachbearbeitungsgrund löschen 876
Einsatz von DECT-Telefonen 884
Einschränkungen von System-Leistungsmerkmalen 882
Konfiguration 836
mehrfache Nachbearbeitung, Nachbearbeitungsgrund ändern 878
mehrfache Nachbearbeitung, Nachbearbeitungsgrund hinzufügen 877
mehrfache Nachbearbeitung, Nachbearbeitungsgrund löschen 878
myAgent 810
myReports 813
myReports Benutzerrollen 814
Nachbearbeitung 830
Nachbearbeitungsgründe 830
Pause 821
Pause ändern 874
Pause hinzufügen 874
Pause löschen 875
Pilot für eingehende Faxnachrichten konfigurieren 870
Regel als PDF-Datei speichern 862
Regel ausdrucken 862
Regel-Editor 768, 824
Rückfalllösung 833
Servicegrad 831
Sollwert für Servicegrad festlegen 870
Teilnehmer als Agent konfigurieren 854
UCD-Gruppe konfigurieren 853
Urlaubsplan 768, 824
VIP-Anruferpriorität 832
VIP-Anruferpriorität festlegen 871
VIP-Rufliste 832
VIP-Rufliste bearbeiten 872
vordefinierte Berichtsvorlagen 886
Vorgehensweise bei der Konfiguration 853
Wandanzeige/Wallboard 831
Warteschlange 822
Warteschlange aktivieren 869
Warteschlange ändern 866
Warteschlange deaktivieren 869
Warteschlange hinzufügen 863
Zeitplan 767, 823
Zeitplan ändern 860
Zeitplan hinzufügen 856
Zeitplan löschen 861
Contact Center, Experten-Modus 1598
Cordless
Basisstationen, Experten-Modus 1548
Multi-SLC, Experten-Modus 1547
SLC, Experten-Modus 1546
Systemweit, Experten-Modus 1544
Cordless-Lösung
Systemausbau 908
Cordless-Telefone 84
Corporate Network 713
Cover Page Editor 547
CRL (Certificate Revocation Lists) 949, 973
CSP (CSTA Service Provider) 1619
CSTA Message Dispatcher (CMD) 1619
CSTA-Protokoll 1132
CSTA Service Provider (CSP) 1619
CSV-Datei 391

D

Darstellungskonventionen 45
Das 560
Datei-Upload, Experten-Modus 1606
Datenschutz 61, 886
Datensicherheit 61
Datensicherung (siehe Sichern)
Datum und Uhrzeit, Experten-Modus 1455
DECT Teilnehmer, Experten-Modus 1527
DECT-Telefone 84
Default Router 323
konfigurieren 324
Default Router, Experten-Modus 1499, 1500
Deployment- und Licensing-Client (DLSC), Experten-Modus 1463
DeskSharing 904
Desktop-Wahl 480, 519
Devices, Experten-Modus 1582

Device-Statistiken, Experten-Modus 1586
DHCP Modus, Experten-Modus 1491
DHCP-Relay-Agent
konfigurieren 315
Diagnosedaten 1256
herunterladen 1258
Diagnose Log 1285
herunterladen 1290
löschen 1290, 1291
öffnen 1290
Diagnose Logs, Experten-Modus 1420
Diagnose-Protokoll 1256
herunterladen 1258
Diagnose-Protokolle, Experten-Modus 1426
Dial In Control Server 714
Dienste sperren (nur LX) 930
Digitale Prüfschleife 1260
Digitale Prüfschleife, Experten-Modus 1409
Digitale Signatur 948
Direktansprechen 569
Direktansprechen für Gruppen 669
Direktansprechschutz für Teilnehmer 569
aktivieren 569
deaktivieren 569
Direktantworten 569
Direktruftaste 568
DISA, Experten-Modus 1444
Diskretes Ansprechen 583
Display, Experten-Modus 1442
DLSC CA -Zertifikat, Experten-Modus 1464
DLSC Client-Zertifikat, Experten-Modus 1463
DLS Notification, Experten-Modus 1428
DNS (Domain Name Service)
Server festlegen 323
DNS-Name 345
DNS-Server 322
DNS-Server, Experten-Modus 1499
Download (siehe Update)
DSL (Digital Subscriber Line) 331
DSP-Kanäle projektieren 1627
DSS-Server 1620
DSS-Taste 568
Dual-Mode-Telefonie 898
Durchsage an Gruppe 669
Gespräch übergeben 670
Durchwahl Rufnummern, Experten-Modus 1541
DynDNS 321
DynDNS (Dynamic Domain Name Service) 345
DynDNS-Service 345
konfigurieren 346, 366, 367, 368, 920
DynDNS Service, Experten-Modus 1452

E

E.164-Nummerierung 998
Editieren der Wahl 561
E-Mail
Benachrichtigung 474, 551
E-Mail, Experten-Modus 1419
E-Mail to SMS 553
E-Mail-Versand 551
Entsorgung 57
Erlaubnisliste anzeigen 691
Erlaubnislisten, Experten-Modus 1574
ESP-Header 937
Euro-ISDN-Leistungsmerkmale 1623
Event (Ereignis) 1283
E-Mail-Einstellungen 1285
E-Mail-Einstellungen ändern 1287
Log-Einträge 1284
Protokolldatei 1284
Protokoll herunterladen 1286
Protokollierung über LAN ändern 1286
Protokoll löschen 1287
Reaktionseinstellungen eines Events ändern 1288
Reaktionseinstellungen mehrerer Events ändern 1289
Reaktionstabelle 1285
Reaktionstabelle anzeigen 1287
Event-Konfiguration, Experten-Modus 1418
Event-Protokoll, Experten-Modus 1419
Events
Alarm-Signalisierung, Experten-Modus 1421
Diagnose Logs, Experten-Modus 1420
E-Mail, Experten-Modus 1419
Event-Konfiguration, Experten-Modus 1418
Event-Protokoll, Experten-Modus 1419
Reaktionstabelle, Experten-Modus 1419
Events, Experten-Modus 1418
Event Viewer 1261
Protokoll ändern 1270
Protokoll anzeigen 1270
Protokoll herunterladen 1270
Protokoll löschen 1271
Protokoll öffnen 1270
EVM, Experten-Modus 1528
Experten-Modus, Experten-Modus 1392
Externes Verzeichnis 508
Externes Verzeichnis, Experten-Modus 1597
Externes Verzeichnis (LDAP) 511

F

FastViewer 534
Favoritenliste 516
Sofortnachricht 475

Favoritenliste (UC Smart) 462
Fax 537
T.38 555
Fax Printer 547
Faxbox 546
Faxbox-Gruppe 663
ändern 667
anzeigen 667
konfigurieren 666, 668
Mitglied hinzufügen 668
Mitglied löschen 668
Faxgruppe (siehe Faxbox-Gruppe)
Fax Gruppe 3 411
Fax Gruppe 4 407
Faxkopfzeilen, Experten-Modus 1614
Fax-Nachrichten 801
Faxnachrichten 537
Fax Printer 480
Fernzugriff auf das Kommunikationssystem 1321
Feste Rufweiterschaltung 584
Firewall 921, 1160
Flex Call 605
Flexible Menüs, Experten-Modus 1450
FTP-Server, Experten-Modus 1491
Funkstörung 61
Funktionen
myPortal 478
myPortal for OpenStage 455, 481
myPortal for Outlook 480
myPortal Smart 454
myPortal for Mobile 888, 889
Funktionstasten 413
programmieren 414, 452, 453, 458, 474

G

Garbage Collection, Experten-Modus 1427
Gate View 1617
Gateway, Experten-Modus 1451
Gebühren Ausgabe, Experten-Modus 1457
Gebühren Faktoren, Experten-Modus 1458
Gebühren Projekt Kennzahlen, Experten-Modus 1459
Geplante Konferenz 530
geplante Konferenz 530
Gesprächsübernahme von Sprachbox 537
Gigaset-Telefone 84
Globale Parameter, Experten-Modus 1492
Grundeinstellungen
Datum und Uhrzeit, Experten-Modus 1455, 1456
DynDNS, Experten-Modus 1452, 1453
Gateway, Experten-Modus 1451
Gebühren, Experten-Modus 1457, 1458, 1459
Port-Verwaltung, Experten-Modus 1456
Power Management, Experten-Modus 1461
Quality of Service, Experten-Modus 1454
System, Experten-Modus 1431, 1436, 1442, 1444, 1445, 1448, 1449, 1450, 1451
Telefonparameter, Experten-Modus 1460
Wiedergabegerät, Experten-Modus 1460
Grundeinstellungen, Experten-Modus 1431, 1616
Gruppen 609
Gruppen, Experten-Modus 1596
Gruppen-/Sammelanschluss, Experten-Modus 1549
Gruppenruf 611
Anklopfschutz für Gruppenmitglied 612
Anklopfschutz für Gruppenmitglied ausschalten 632
Anklopfschutz für Gruppenmitglied einschalten 632
Rufart 614
SIP-Telefone 614
Sprachbox 612
Typ Anklopfen, Mitglied hinzufügen 632
Typ Anklopfen, Mitglied löschen 632
Typ Anklopfen ändern 631
Typ Anklopfen anzeigen 631
Typ Anklopfen hinzufügen 630
Typ Anklopfen löschen 631
Typ Freifall, Mitglied hinzufügen 632
Typ Freifall, Mitglied löschen 632
Typ Freifall ändern 631
Typ Freifall anzeigen 631
Typ Freifall hinzufügen 630
Typ Freifall löschen 631
Typ Gruppe, Mitglied hinzufügen 623
Typ Gruppe, Mitglied löschen 623
Typ Gruppe ändern 622
Typ Gruppe hinzufügen 620
Typ Gruppe löschen 623
Gruppen-Teilnehmer, Experten-Modus 1551

H

H.323-Stack-Trace 1263
Konfiguration ändern 1275
Konfiguration anzeigen 1275
Module ändern 1275
Protokoll herunterladen 1276
Protokoll löschen 1276
Protokoll öffnen 1276
H.323-Stack-Trace, Experten-Modus 1414
Halten 578
Handlungsanweisung 45
Hardware-Konfiguration OpenScape Office MX anzeigen 450
Hardwaretausch 304
Hauptnetzanbieter 713

Herunterfahren von OpenScape Business X 1228
Hinweise zur gleichzeitigen Nutzung von myAgent und UC Suite Clients 818
Host-Name, Experten-Modus 1485, 1496
HotDesking 904
Hotline 750
HW-Module, Experten-Modus 1583

I

ICMP (Internet Control Message Protocol) 1249
IKE-SA 947
Image-Datei 1211
Installation 106, 188, 238
Instant Message 475, 557
Instant Messaging 801
Internes Verzeichnis (UC Smart) 461
Internes Verzeichnis (UC Suite) 507
Internet-Modem 336
Internet-Router 333
Internet-Telefonie 350
Internet-Telefonie Service Provider, Experten-Modus 1514
Internet-Telefonie-Service-Provider (ITSP) 150, 210, 350, 352
Internet-Zugang 331
  Konfiguration 332
  über externen Internet-Router 333
  über externes Internet-Modem 336
  über Standard-ISP PPPoE konfigurieren 340
  über Standard-ISP PPTP konfigurieren 343
  über vorkonfigurierten ISP konfigurieren 337
Interne Wartemusik 1191, 1193
Inventory-Management 1233
Inventory OpenScape Business S 1240
  abfragen 1242
Inventory OpenScape Business X 1239
Inventory OpenScape Business X3/X5/X8
  abfragen 1240
Inventory OpenScape Office LX/HX
  abfragen 309
Inventory OpenScape Office MX
  abfragen 308
IP-Adressen 1234
  Übersicht anzeigen 1238
IP-Adressen-Pools, Experten-Modus 1493
IP-Adressen-Schema 110, 192
IP-Client (siehe IP-Teilnehmer)
IP Clients, Experten-Modus 1523, 1543
IP-Diagnose
  Mainboard, Experten-Modus 1429, 1430
IP-Diagnose, Experten-Modus 1429
IP-Gateway-Adresse, Experten-Modus 1398
IP-Mobility 904
IPSec-Tunnel 946
IP-Teilnehmer 402
ISDN-Amtsleitung
  gezielte Belegung 714
ISDN-Amtszugang konfigurieren 370
ISDN-Karte 407
ISDN-Modem 407
ISDN-Parameter, Experten-Modus 1571
ISDN-Teilnehmer 407
ISDN Teilnehmer, Experten-Modus 1525
ISDN-Telefon 407
ITSP (Internet-Telefonie-Service-Provider) 350
ITSP-Status 1233
  abfragen 1236
IVM 1618
IVM, Experten-Modus 1528

J

Java 1160
Java Runtime Environment (JRE) 107, 189
Journal
  Aufbewahrungsdauer 516
Journal (UC Smart) 462
Journal (UC Suite) 516

K

Kabelanschluss 332
kanonisches Rufnummernformat 463
Kapazitäten 1374
Keypad-Wahl 560
Knoten, Experten-Modus 1518
Kommende Rufe
  Anrufübernahme, Experten-Modus 1555
  Gruppen-/Sammelanschluss, Experten-Modus 1549
  Gruppen-Teilnehmer, Experten-Modus 1551
  Rufweiterschaltungen, Experten-Modus 1558
  Team/Top, Experten-Modus 1552
  UCD, Experten-Modus 1556
Kommende Rufe, Experten-Modus 1548
Kommunikationssystem herunterfahren 1228
Konferenz 522
  AdHoc- 529
  Applikationsgesteuert 522
  Arten von Konferenzen 522
  Aufzeichnung 522
  Authentifizierung 522
  automatische Einladung per E-Mail 522
  automatische Einladung per Outlook-Termin 522
  Einwahlnummer 522
  geplante 530

Konferenzleiter 522
Konferenzteilnehmer 522
Konferenzton 522
Mobility-Entry-Teilnehmer 522, 529, 530, 531, 532
offene 532
permanente 531
Telefongesteuert 522
Verlängerung 522
Virtueller Konferenzraum 522
Konferenz (UC Smart) 464
Konferenz (UC Suite) 522
Konferenz-Management 523
Konferenzschaltung, Experten-Modus 1607
Konferenzton aktivieren / deaktivieren 589, 590
Konfiguration
Ansagen, Experten-Modus 1394
Branding, Experten-Modus 1398
IP-Gateway-Adresse, Experten-Modus 1398
Port-Konfiguration, Experten-Modus 1394
SmartVM, Experten-Modus 1395, 1396
Wartemusik (MoH), Experten-Modus 1393
Konfiguration, Experten-Modus 1393, 1425
Konfiguration externe Anbieter, Experten-Modus 1597
Konfigurationsdaten 1201
Konfigurationsdaten für die Diagnose 1291
erzeugen 1292
Konfigurierte Dienste, Experten-Modus 1472
Konfigurierte Regeln, Experten-Modus 1480
Konfigurierte Tunnel, Experten-Modus 1475
Konfigurierte Zertifikate, Experten-Modus 1470
Konformität
internationale Normen 63
US- und kanadische Normen 63
Kontakt 516
Konzept 45
Kunden-Trace-Protokoll 1261
ändern 1270
anzeigen 1270
herunterladen 1270
löschen 1271
öffnen 1270
Kunden-Trace-Protokoll, Experten-Modus 1409
Kurzwahlen, Experten-Modus 1616
Kurzwahl individuell (KWI) 567
Kurzwahl zentral (KWZ) 564
Kurzwahlziele, Experten-Modus 1450

L

Laden zum Gateway, Experten-Modus 1393, 1394
LAN 1, Experten-Modus 1496
LAN 1 (WAN), Experten-Modus 1485
LAN 2, Experten-Modus 1489, 1497
LAN 3 (Admin), Experten-Modus 1490
LAN-Anforderungen 993
Lautsprecher 411
LCR
Classes Of Service, Experten-Modus 1507
LCR-Flags, Experten-Modus 1506
Wahlplan, Experten-Modus 1507
Wahlregel, Experten-Modus 1509
Wegetabelle, Experten-Modus 1508
LCR (Least Cost Routing) 702
Berechtigung 710
Berechtigung vergeben/ändern 710
Funktionalität 703
Wahlplan 706
Wahlplan bearbeiten 707
Wahlregeln 711
Wahlregeln bearbeiten 712
Wegetabelle 708
Wegetabelle bearbeiten 709
LCR-Flags, Experten-Modus 1506
LCR Least Cost Routing
Funktionalität 703
LDAP, Experten-Modus 1448
LDAP-Verbindung 1160
Leistungsmerkmale
Voice, netzweit 991
Leitungen 369
Belegungsart 376
Belegungsart konfigurieren 380, 385, 387
Kennzahl ändern 373
MSN zuweisen 374
Protokoll ändern 374, 375
Richtung ändern 379
Leitungen, Experten-Modus 1561
Leitungen/Vernetzung
ISDN-Parameter, Experten-Modus 1571
Leitungen, Experten-Modus 1561
MSN zuweisen, Experten-Modus 1571
QSIG-Leistungsmerkmale, Experten-Modus 1570
Richtung, Experten-Modus 1563
Leitungen/Vernetzung, Experten-Modus 1560
Leitungstrennung für einen Notruf 752
Leitungsvormerken 570
Lesende Communities, Experten-Modus 1423
Lightweight-CA 949
Lightweight CA, Experten-Modus 1468
Lizenz 264
aktualisieren 305
Informationen anzeigen 296, 297, 298, 299, 309
über Lizenz-Autorisierungscode aktivieren 277, 1344
über Lizenzdatei aktivieren 277

Lizenzaktivierung 275, 286
Lizenzaktualisierung 304
Lizenz-Autorisierungscode (LAC) 275, 286
Lizenzdatei 275, 286
Lizenz-Komponenten-Trace 1263
ändern 1277
Lizenz-Komponenten-Trace, Experten-Modus 1415
Lizenzserver (CLS) 305
IP-Adresse ändern 177, 227, 281, 283, 292, 294, 300, 301, 302, 303, 306
LXV3, Experten-Modus 1617

M

M5T-Trace-Komponente 1261
ändern 1272
anzeigen 1271
starten 1272
stoppen 1272
M5T-Trace-Komponenten, Experten-Modus 1410
Mail-Exchange-Eintrag 345
Mail Exchanger 346
Mail-Exchanger 345
definieren 349
Mainboard, Experten-Modus 1429
Makeln 579
Manager E 103
Manuelle Aktion 1256
Mapping (Anwesenheitsstatus UC Suite) 499
MCL Single Stage 713
MCL Two Stage 713
MEB (Media Extension Bridge) 1620
Media Extension Bridge (MEB) 1620
Media Stream Control (MSC), Experten-Modus 1583
Mediatrix 4102S 84
Medium, Backup (siehe Backup-Medium)
Mehrsprachige Textausgabe 1190
Mitteilungstexte 600
Mobile Pin 605
Mobiles Logon 904
Mobile User Logon 904
Mobility
Mobiltelefon für GSM konfigurieren 900
Teilnehmer löschen 904
Mobility Entry 893
Leistungsmerkmal-Codes 893
Mobility Entry, Experten-Modus 1542
Mobility-Entry-Teilnehmer
Konferenz 522, 529, 530, 531, 532
Mobiltelefon 890
Modem 411
MoH 1191, 1193
MSC-Statistiken, Experten-Modus 1587
MSN zuweisen, Experten-Modus 1571
Multi Location 985
Multi-SLC, Experten-Modus 1547
Multi User Chat 1157
MX-Record 345
myAgent
Voraussetzungen 811
myPortal
Funktionen 478
Präsenz-Status 478
myPortal for Mobile 888
Funktionen 888, 889
myPortal for OpenStage
Anwesenheitsstatus 455, 481
Funktionen 455, 481
myPortal for Outlook
Funktionen 480
myPortal Smart
Funktionen 454
myPortal for Mobile
Anwesenheitsstatus 888
myPortal to go
Voraussetzungen 892
myReports
Administrator-Kennwort zurücksetzen 815
Benutzerrollen 814

N

Nachrichten
verwalten 801
Nachrichtenübersicht 801
Nacht
Berechtigungsgruppen, Experten-Modus 1573
Nachtschaltung, Experten-Modus 1575
Nachwahl 564
NAT, Experten-Modus 1501
NAT (Network Address Translation) 924
NAT-Regel 924
konfigurieren 925
löschen 927
mit NAT-Tabelleneditor konfigurieren 926
NAT-Tabelleneditor 926
NCP-Client
aktivieren, deaktivieren 958
vorbereiten 958
Netzanbieter 713
Netzwerk
Lizenz 992
Netzwerkparameter (LAN, WAN) 993
Netzwerkschnittstellen
Applicationboard, Experten-Modus 1496, 1497

Mainboard, Experten-Modus 1485, 1489, 1490, 1491, 1492, 1493, 1494, 1495, 1496
Netzwerkschnittstellen, Experten-Modus 1485
Netzwerkverbindung prüfen 1249
über Ping 1249
über Traceroute 1250
Neustart der UC Applikation 1231
Neustart der UC Booster Card 1229
Neustart der Web Services 1232
auslösen 1232
Neustart von OpenScape Business 1225
Notfallverhalten 56
Notrufdienst E911 752
Notrufe
Voraussetzungen 749
Nummerierung
offene 997
verdeckt, geschlossen 997

O

Offene Konferenz 532
Öffentliche Rufnummern im Netz 998
Online Benutzer 1430
Online-Benutzer 1328
starten 1248, 1328
Online-Benutzer, Experten-Modus 1430
Open Directory Service 1149, 1160
Datenquellen, Experten-Modus 1616, 1617
Grundeinstellungen, Experten-Modus 1616
Wartung, Experten-Modus 1617
Open Directory Service, Experten-Modus 1616, 1617
OpenScape Business X3R
Schutzerdung 1339, 1340, 1342
OpenScape Business X5R
Schutzerdung 1339, 1340, 1342
OpenScape Business Assistant 88, 90
OpenScape Business Cordless (siehe Cordless-Lösung)
OpenScape Office, Experten-Modus 1616
OpenScape Personal Edition 84
OpenStage 84
OpenStage Attendant 778
OpenStage Gate View 1115
optiPoint 84
Out of Service, Experten-Modus 1406

P

Padding 937
Paging Intern 669
Parken 578
Päsenz (UC Smart) 459
Path Replacement 998
Payload
Devices, Experten-Modus 1582
HW-Module, Experten-Modus 1583
Media Stream Control (MSC), Experten-Modus 1583
Payload, Experten-Modus 1582
Payload-SA 947
PC-Clients 84
PDF-Datei
Benachrichtigung 551
Faxnachricht 546
Peer-Zertifikate, Experten-Modus 1470
Permanente Konferenz 531
Ping, Experten-Modus 1429
PIN zur Aktivierung eines Shutdowns 1229
PKI-Server
anzeigen 972
hinzufügen 972
Plattform-Diagnose, Experten-Modus 1428
Port 1160
Port-, Baugruppen-Zustand, Experten-Modus 1405
Port-Konfiguration, Experten-Modus 1394
Ports 922
Portfreigabe konfigurieren 923, 1097
Portverwaltung 923
Port-Verwaltung, Experten-Modus 1456
Power Management, Experten-Modus 1461
PPP-Protokoll, Experten-Modus 1502
Präsenz (UC Suite) 499
Präsenz-Status 455, 478, 481
Presence (UC Smart) 459
Presence (UC Suite) 499
Pre-shared Keys 947
Primary Rate Interface 714
Priorisierungsklassen 399
Priorisierung von Amtsleitungen 387
Privatleitung 571
Profile
alle Profile exportieren 445, 919
alle Profile importieren 445, 919
ändern 444
einzelnes Profil exportieren 443
einzelnes Profil importieren 443
Mitglieder anzeigen 441
Mitglieder hinzufügen 441
Mitglieder löschen 442
neu anlegen 440
Profile anzeigen 441
Profile, Experten-Modus 1612
Profile/Vorlagen, Experten-Modus 1540
Profil für Konfigurationsdaten von Application Launcher 1160

Prolile
Teilnehmer 439
PSTN, Experten-Modus 1502
PSTN-Partner, Experten-Modus 1502
Public Instant Messaging 1157
Public Key Infrastructure (PKI), Experten-Modus 1481

Q

QSIG-Leistungsmerkmale, Experten-Modus 1570
Quality of Service, Experten-Modus 1454
Quality of Service (QoS) 399
konfigurieren 401

R

RAS-User 402
Reaktionstabelle, Experten-Modus 1419
Recycling 57
Regel 503
Reload der UC Booster Card 1230
Reload von OpenScape Business 1226
Relocate 605
Remote Services 1310
Remote-Zugang 1321
ausschalten 1327
einschalten, über Internet-Zugang mit fester IP-Adresse 176, 179, 180, 181, 226, 228, 230, 1325
einschalten, über Internet-Zugang ohne feste IP-Adresse 1326
einschalten, über ISDN 1322
PC konfigurieren 1322
PC mit Windows 7 konfigurieren 1324
Restart / Reload
Restart / Reload, Experten-Modus 1422
Restart / Reload, Experten-Modus 1421, 1422
Restart der UC Applikation 1231
Restart der UC Booster Card 1229
Restart der Web Services 1232
auslösen 1232
Restart von OpenScape Business 1225
Restore (siehe Wiederherstellen)
R-Gesprächsschutz je Amtsleitung 702
Richtung, Experten-Modus 1563
Richtungen 369, 375
Anlagenrufnummer eintragen 381
Kennzahl zuweisen 380
Namen zuweisen 379
Nr.-Typ gehend konfigurieren 382
Präfix ergänzen kommend 377, 382
Rufnummerntyp konfigurieren 382
Überlaufrichtung eintragen 380
Zweite Amtskennzahl eintragen 383
Röchelschaltung 750
Routing 323
IP-Routing, Experten-Modus 1498, 1499, 1500
NAT, Experten-Modus 1501
PSTN, Experten-Modus 1502
Routing, Experten-Modus 1498, 1518
RPCAP-Dämon 1282
aktivieren 1283
deaktivieren 1283
rpcap Dämon, Experten-Modus 1417
Rückruf 595
Journal 516
Rückruf bei Besetzt 596
Rufeinblendung/Anklopfen 596
Rufnummern
importieren 394
Rufnummernformat 463
Rufnummernplan 109, 192, 389
ändern 393
importieren 394
löschen 392
Rufnummerntausch 605
Rufnummernübermittlung des Angerufenen - COLP 575
Rufnummernübermittlung des Anrufers - CLIP 572
Rufnummernumwertung in Namen 577
Rufnummernunterdrückung des Angerufenen - COLR 575
Rufnummernunterdrückung des Anrufers - CLIR 574
Rufsignalisierungen 572
Rufweiterschaltungen, Experten-Modus 1558
Rufweiterschaltung im Amt 591
Rufweiterschaltung im Besetztfall 585
Rufweiterschaltung konfigurieren 468, 586
Rufweiterschaltung nach Zeit 584
Rufzuordnung 591
Rufzuschaltung 592

S

Sammelanschluss 615
ändern 625
hinzufügen 624
löschen 627
Mitglied hinzufügen 627
Mitglied löschen 627
Rufart 617
SIP-Telefone 617
Sprachbox 616
Schreibende Communities, Experten-Modus 1424
Secure Trace 1261
Passphrase ändern 1274
Passwort ändern 1274

starten 1273
Status abfragen 1273
stoppen 1273, 1274
X.509-Datei importieren 1274
Zertifikat aus X.509-Datei importieren 1274
Secure Trace, Experten-Modus 1410
Secure Trace-Einstellungen, Experten-Modus 1411
Secure Trace-Zertifikat, Experten-Modus 1411
Security Associations SA 947
Security Checklist 921
Sekretär-Funktion (siehe Chef/Sekretär-Konfiguration)
Server, Experten-Modus 1608
Server-Zertifikate, Experten-Modus 1483
Service Codes, Experten-Modus 1451
Servicekennzahlen, Experten-Modus 1451
Shutdown
PIN zur Aktivierung 1229
Sicherheit
Application Firewall, Experten-Modus 1462
Deployment- und Licensing-Client (DLSC), Experten-Modus 1463, 1464
Signaling- und Payload-Encryption, Experten-Modus 1465, 1466, 1467
SSL, Experten-Modus 1481, 1483
VPN, Experten-Modus 1467, 1468, 1469, 1470, 1472, 1473, 1475, 1479, 1480, 1481
Web Sicherheit, Experten-Modus 1484
Sicherheit, Experten-Modus 1462
Sicherheitshinweise 45
Sicherheitshinweise für Australien 51
Sicherheitshinweise für Brasilien 52
Sicherheitshinweise für Kanada 55
Sicherheitshinweise für USA 52
Sichern 1201
sofort 1207
zeitgesteuert 1208
Signaling and Payload Encryption
SPE Unterstützung aktivieren 933
SPE Unterstützung deaktivieren 933
Signaling and Payload Encryption SPE 930
Signaling- und Payload-Encryption, Experten-Modus 1465
Single Location 985
SIP-Client 402
SIP Interconnection, Experten-Modus 1519
SIP-Parameter, Experten-Modus 1511
SIP-Telefone 84
Site Of Operations, Experten-Modus 1591
Skin-Einstellungen, Experten-Modus 1614
SLC, Experten-Modus 1546
Smartphone 890
Sma rtVM, Experten-Modus 1395
SmartVM, Experten-Modus 1395, 1396, 1579
SMS
Benachrichtigung 551
SMS-Benachrichtigung 553
SMS-Template 553
SNMP
Communities, Experten-Modus 1423, 1424
Traps, Experten-Modus 1424
SNMP, Experten-Modus 1423
SNMP (Simple Network Management Protocol) 1250
Communities 1251
Communities anzeigen 1252
Community ändern 1254
Community hinzufügen 1253
Community löschen 1254
Management-Informationsdatenbank MIB 1251
Trap-Detaildaten anzeigen 1255
Traps 1251
Traps anzeigen 1254
SNMP Statistik, Experten-Modus 1587
SNTP-Einstellungen, Experten-Modus 1456
Sofortnachricht 475, 557
Sofortnachrichten 801
Software-Aktivierung 1210
Software-Aktualisierung 1210
Software-Image
System-Software, Experten-Modus 1399, 1400
Software-Image, Experten-Modus 1399, 1403
Software-Übertragung 1210
Software-Update (siehe Update)
Sondertage, Experten-Modus 1578
SPE CA Zertifikate, Experten-Modus 1467
SPE Zertifikat, Experten-Modus 1466
Sprachbox 537
Gesprächsübernahme 537
statusbezogene Ansagen 537
Sprachbox (UC Smart) 466
Sprachbox-Gruppe 662
ändern 664
anzeigen 664
hinzufügen 664
löschen 665
Mitglied ändern 666
Mitglied hinzufügen 665
Mitglied löschen 665
Sprachen 85
Sprachgateway
Codec-Parameter, Experten-Modus 1512
Internet-Telefonie Service Provider, Experten-Modus 1514
Networking, Experten-Modus 1518
SIP Interconnection, Experten-Modus 1519

SIP-Parameter, Experten-Modus 1511
Ziel-Codec-Parameter, Experten-Modus 1514
Sprachgateway, Experten-Modus 1511
Sprachnachricht 537
speichern 537
Sprachnachrichten 537, 801
Sprachnachrichten (UC Smart) 466
SSDP (Smart Services Delivery Platform) 1310
Geräte verwalten 1319
Partner-ID ändern 1319
PIN zur Aktivierung/Deaktivierung des Service-Plugin konfigurieren 1320
Service-Plugin deaktivieren 1317
Service-Plugin konfigurieren für ein Kundennetz mit Proxy 1313, 1315
Service-Plugin registrieren für ein Kundennetz mit Proxy 1315
Service-Plugin zurücksetzen 1318
SSL (Secure Socket Layer) 973
CA-Zertifikat generieren 974
Selbstsigniertes Zertifikat generieren 974
Server-Zertifikat importieren 975
Verlängertes Zertifikat importieren 977
Zertifikat aktivieren 978
Zertifikate anzeigen 928, 929, 976
Zertifikat exportieren 977
Zertifikat löschen 976
Zertifikatsanforderung generieren 975
Standards 1621
Standort-Liste, Experten-Modus 1608
Statische IP-Adressen, Experten-Modus 1494
Statische Routen 323
hinzufügen 324, 328, 329
löschen 325
Statische Routen, Experten-Modus 1498, 1500
Statistiken
Gateway-Statistk, Experten-Modus 1586
Gateway-Statistken, Experten-Modus 1587
SNMP Statistik, Experten-Modus 1587
Telephonie Statistiken, Experten-Modus 1587, 1588, 1589
Statistiken, Experten-Modus 1586
statusbezogene Sprachbox-Ansagen 537
Status des Kommunikationssystems 1233
Störaussendung 61
STUN (Simple Traversal of UDP through NAT) 367
Survivability 1097
System-Client 402
System-Flag
Anrufübernahme nach Wiederanruf 630, 999
A-Rufnummer in AUN-Gruppen / Rufzuschaltung / Umleitungsziel / RWS-Ziel 628
Aufmerksamkeitssignalisierung bei AUN-Gruppen 629
SPE Unterstützung 933
System Flags, Experten-Modus 1431
Systemsprache für Sprachbox 537
Systemtelefonbuch 462
Systemtelefonbuch (UC Suite) 514
System Texte, Experten-Modus 1587
Systemverbindung 1160
Systemweit, Experten-Modus 1544

T

T.38-Fax 555
Tablet-PC 890
Tag
Berechtigungsgruppen, Experten-Modus 1573
Tastenkombination für Desktop-Wahl 519
Tastenprogrammierung 413
Tastenprogrammierung, Experten-Modus 1544
TCP-Dump 1281
löschen 1282
starten 1281
stoppen 1281
TCP- Dump, Experten-Modus 1417
Team (siehe Teamschaltung)
Team/Top, Experten-Modus 1552
Teamfunktion (siehe Teamschaltung)
Team-Gruppe 633
ändern 642
Eigenschaften eines Mitglieds ändern 647
Faxbox 635
Faxbox hinzufügen 648
hinzufügen 641
löschen 643
Mitglied ändern 647
Mitglied hinzufügen 646
Mitglied löschen 646
Rufart 635
SIP-Telefone 636
Telefon-Tastenbelegung ändern 648
Teamschaltung 633
ändern 642
Eigenschaften eines Mitglieds ändern 647
Faxbox 635
Faxbox hinzufügen 648
hinzufügen 641
löschen 643
Mitglied ändern 647
Mitglied hinzufügen 646
Mitglied löschen 646
Rufart 635
SIP-Telefone 636

Telefon-Tastenbelegung ändern 648
Teilnehmer 389
analog 411
IP 402
ISDN 407
Konfiguration über Wizards 417
Tastenprogrammierung, Experten-Modus 1544
Teilnehmer, Experten-Modus 1520, 1523, 1524, 1525, 1526, 1527, 1528, 1529, 1530, 1539, 1540, 1541, 1542
Übersicht, Experten-Modus 1543
Teilnehmer, Experten-Modus 1520, 1572, 1589
Teilnehmerdaten
importieren 394
Teilnehmer-Flag
Anklopfschutz ein 632
Direktansprechschutz aus 569
Teilnehmer-Parameter, Experten-Modus 1530
Teilnehmer-Profile 439
Teilnehmer-Status 1233
abfragen 1234
Telefon abschließen 701
Telefone 84
Telefongespräche übergeben 580
Telefongesteuerte Konferenz 523
Telefonie, Experten-Modus 1431
Telefon-Image
Laden, Experten-Modus 1401
Verteilen pro Endgerät, Experten-Modus 1402
Telefon-Images
Verteilen, Experten-Modus 1401
Telefon-Logo
Laden, Experten-Modus 1402
Verteilen, Experten-Modus 1403
Telefonparameter, Experten-Modus 1460
Teleworking 502, 916
Templates, Experten-Modus 1596
Termin 608
Terminalserver-/Citrix-Server-Umgebungen 478
Texts, Experten-Modus 1449
Themen, Arten 45
TIFF-Datei
Benachrichtigung 551
Faxnachricht 546
Top-Gruppe 636
ändern 644
Eigenschaften eines Mitglieds ändern 650
Faxbox 639
Faxbox hinzufügen 650
hinzufügen 643
löschen 645
Mitglied ändern 649
Mitglied hinzufügen 649
Mitglied löschen 649
Rufart 639
SIP-Telefone 639
Trace 1259
Ausgabe-Interfaces 1260
Ausgabe-Interfaces ändern 1269
Ausgabe-Interfaces anzeigen 1269
Format-Konfiguration 1259
Format-Konfiguration ändern 1269
Format-Konfiguration anzeigen 1269
Protokoll 1260
Protokoll herunterladen 1266
Protokoll löschen 1267
Trace-Ausgabe-Interfaces, Experten-Modus 1408
Trace-Format-Konfiguration, Experten-Modus 1407
Trace-Komponente 1265
alle Komponenten stoppen 1280
ändern 1280
anzeigen 1279
Detaildaten anzeigen 1279
starten 1279
stoppen 1279
Trace-Komponenten, Experten-Modus 1416
Trace-Konsolen-Ausgabe, Experten-Modus 1429
Trace-Profil 1264
alle Profile stoppen 1278
anzeigen 1267
Detaildaten anzeigen 1277
hinzufügen 1278
starten 1268
stoppen 1268
Trace-Profile, Experten-Modus 1416
Trace- Protokoll, Experten-Modus 1409
Traceroute, Experten-Modus 1430
Traces
Call Monitoring, Experten-Modus 1412
Digitale Prüfschleife, Experten-Modus 1409
H.323-Stack-Trace, Experten-Modus 1414
Kunden-Trace-Protokoll, Experten-Modus 1409
Lizenz-Komponente, Experten-Modus 1415
M5T-Trace-Komponenten, Experten-Modus 1410
rpcap Dämon, Experten-Modus 1417
Secure Trace, Experten-Modus 1410, 1411
TCP- Dump, Experten-Modus 1417
Trace-Ausgabe-Interfaces, Experten-Modus 1408
Trace-Format-Konfiguration, Experten-Modus 1407
Trace-Komponenten, Experten-Modus 1416
Trace-Profile, Experten-Modus 1416
Trace- Protokoll, Experten-Modus 1409
Traces, Experten-Modus 1407

Trap Communities, Experten-Modus 1424
Traps, Experten-Modus 1424
Türsprechstelle, Experten-Modus 1579
Türsprechstelle/Türöffner 1108

U

Übergabe an Gruppe aus Durchsage 669
Übermittlung kundenspezifischer Rufnummerninformation 576
Übernahme des Write Tokens, Experten-Modus 1429
Übertragung, Software (siehe Software-Übertragung)
UC Smart
  Status 1309
  Status abrufen 1309
UC Suite
  Ablagepfad für Client-Log-Dateien konfigurieren 1300
  Aufbewahrungszeit für Contact-Center-Daten konfigurieren 1308
  Aufbewahrungszeit für Protokolldateien konfigurieren 1308
  Aufzeichnung der Client-Logs systemweit aktivieren 1299
  Aufzeichnung der Client-Logs systemweit deaktivieren 1299
  Aufzeichnung der Client-Logs teilnehmerindividuell aktivieren 1300
  Aufzeichnung der Client-Logs teilnehmerindividuell deaktivieren 1300
  Aufzeichnung der Systemprotokolle aktivieren 1298
  Aufzeichnung der Systemprotokolle deaktivieren 1299
  Benachrichtigung 1303
  Client Logs 1298
  Client Logs herunterladen 1302
  E-Mail-Benachrichtigung 1303
  E-Mail-Benachrichtigungen bei Systemfehlern konfigurieren 1305
  Speichern der Client-Logs auf der Festplatte aktivieren 1301
  Speichern der Client-Logs auf der Festplatte deaktivieren 1301
  Systemprotokolle 1297
  Systemwartung sofort durchführen 1308
  Tageszeit für Wartung konfigurieren 1307
  Überwachung 1297
  Wartung 1297, 1306
UCD, Experten-Modus 1556
UCD (Uniform Call Distribution) (siehe Anrufverteilung)
UCD Agenten, Experten-Modus 1588
UC Smart
  Benutzerverwaltung 1592
  Grundeinstellungen 1591
  Status 1593
UC Smart, Experten-Modus 1591
UC Smart Client 454
UC Suite 1593
  Abteilungen, Experten-Modus 1595
  Benutzerverzeichnis, Experten-Modus 1594
  Contact Center, Experten-Modus 1598
  Datei-Upload, Experten-Modus 1606
  Externes Verzeichnis, Experten-Modus 1597
  Faxkopfzeilen, Experten-Modus 1614
  Gruppen, Experten-Modus 1596
  Konferenzschaltung, Experten-Modus 1607
  Konfiguration externe Anbieter, Experten-Modus 1597
  Profile, Experten-Modus 1612
  Server, Experten-Modus 1608
  Skin-Einstellungen, Experten-Modus 1614
  Standort-Liste, Experten-Modus 1608
  Templates, Experten-Modus 1596
  Zeitpläne, Experten-Modus 1605
UC Suite, Experten-Modus 1593
UC Suite Clients 477
Umfang für Sprachbox 537
Umleiten nach Zeit 590
Unfall melden 56
UP0 Teilnehmer, Experten-Modus 1520
Update 1210
  benutzerdefiniert 1220
Update, komplett
  im Hintergrund starten 1218
  mit Fortschrittsanzeige starten 1215, 1224
Update via File Upload, Experten-Modus 1400
Update via Internet, Experten-Modus 1399
Update via USB Stick, Experten-Modus 1400
Upgrade 1210

V

VBZ-Gruppen 698
  Leitung zuweisen 700
  Teilnehmer zuweisen 699
  Zuordnung der KWZ-Nummern 699
VBZ Gruppenzuordnung, Experten-Modus 1576
VBZ Matrix, Experten-Modus 1576
VBZ-Matrix ändern 700
VBZ Verkehrsbeziehungen 698
Verbindungsaufbau-Status 1233
  abfragen 1235
Verbindung zum lokalen CLA 294, 295, 307
Verbindung zum zentralen CLA 307
Verbotsliste anzeigen 691

Verbotslisten, Experten-Modus 1575
Verhalten im Notfall 56
Verkabelung für LAN- und WAN-Anschlüsse 59
Vernetzung
homogen, nativ 983
inhomogen, hybrid 983
Knoten aus Netzverbund entfernen 1100
Vernetzungsplan 983
Versorgungsstromkreis und Anschluss
OpenScape Business S 58
OpenScape Business UC Booster Server 58
Verzeichnis
Sofortnachricht 475
Verzeichnisse (UC Smart) 459
Verzeichnisse (UC Suite) 504
Virtuelle Teilnehmer, Experten-Modus 1529
Voice-Mailbox, siehe Sprachbox 537
Voraussetzungen für Application Launcher 1160
Voraussetzungen für myAgent 811
Voraussetzungen für myPortal for Mobile 889
Voraussetzungen für myPortal for OpenStage 456, 485
Voraussetzungen für myPortal to go 892
Voraussetzungen für myReports 816
VPN
Authentifizierung 947
Bandbreiten 937
Clients 954
Sicherheitsmechanismen 946
Zertifikate 949
VPN, Experten-Modus 1467
VPN (Virtual Private Network) 935
End-to-Site 936
Site-to-Site 936
VPN Aktive Dienste
Alle Dienste anzeigen 961
Speziellen Dienst anzeigen 961
VPN Aktive Tunnel
anzeigen 963
Regeln anzeigen 964
VPN Konfigurierte Dienste
Alle Dienste anzeigen 961
ändern 962
löschen 963
umbenennen 962
VPN Konfigurierte Tunnel
anzeigen 965
hinzufügen 966
Regeln anzeigen 965
VPN Regeln
alle aktiven Regeln anzeigen 968
alle konfigurierten Regeln anzeigen 969
ändern 970
hinzufügen für Gegenrichtung 971
konfigurierte Regel hinzufügen 969
löschen 971
spezielle aktive Regel anzeigen 968
VPN-Status 1234
abfragen 1237
VPN-Zertifikate
anzeigen 951
importieren 954
Lightweight-CA-Zertifikat generieren 950
Trusted CA-Zertifikat importieren 952
Zertifikatsanforderung generieren 952, 953

W

Wahlaussendung 705
auswählen 705
wählbares Rufnummernformat 463
Wählpause 567
Wahlplan 706
Wahlplan, Experten-Modus 1507
Wahlregel, Experten-Modus 1509
Wahlregeln 711
Wahlwiederholung 562
WAN 345
WAN-Anforderungen 995
Warnhinweise 46
Gefahr 47
Hinweis 50
Vorsicht 49
Warnung 47
Wartemusik 1191, 1193
Wartemusik (Music On Hold MOH) bei Anrufverteilung 682
Wartung, Experten-Modus 1393, 1617
WAV-Datei
Benachrichtigung 474, 551
Wave-Datei 1191, 1193
WBM 88
Startseite 88
Web-based Management 88
Web Collaboration 534
Web Collaboration, Experten-Modus 1615
Web Services 1160
Web Collaboration, Experten-Modus 1615
XMPP, Experten-Modus 1614
Web Services, Experten-Modus 1614
Web Services Interface 1148
Web Sicherheit, Experten-Modus 1484
Weckeinrichtung 608
Wegeoptimierung 998
Wegetabelle 708

Wegetabelle, Experten-Modus 1508
Weiterleitung, Experten-Modus 1589
Wiederanruf 580
Wiedergabegerät, Experten-Modus 1460
Wiedergabegerät für Ansagen 1618
Wiederherstellen 1201, 1209
Wizards> 96
WLAN-Telefone 84

X

XMPP 1157
XMPP, Experten-Modus 1614

Z

Zeitparameter
Überwachung eines Übergeben vor Melden an eine UCD-Gruppe 683
Überwachung eines UCD-Rufes auf einer analogen Leitung 684
Zeitparameter, Experten-Modus 1436
Zeitpläne, Experten-Modus 1605
Zeitzonen-Einstellungen, Experten-Modus 1455
Zertifikatsgenerierung, Experten-Modus 1481
Zertifikatsverwaltung, Experten-Modus 1468, 1483
Ziel-Codec-Parameter, Experten-Modus 1514
Ziffernwahl 560
Zuletzt aktive Leases, Experten-Modus 1495
Zurückstellen eines Rufes 594
Zustand Leitung, Experten-Modus 1588