



Unify OpenScape Business

OpenScape Business V3

Leistungsmerkmalbeschreibung

A31003-P3030-F100-32-0018

Atos

Senden Sie Ihr Feedback zur Verbesserung dieses Dokumentes an edoku@atos.net.

Als Reseller wenden sich für spezifische Presales-Fragen bitte an die entsprechende Presales-Organisation bei Unify oder Ihrem Distributor. Für spezifische technische Anfragen nutzen Sie die Support Knowledgebase, eröffnen - sofern entsprechender Software Support Vertrag vorliegt - ein Ticket über das Partner Portal oder kontaktieren Ihren Distributor.

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

Copyright © Unify Software and Solutions GmbH & Co. KG 22/02/2024
Alle Rechte vorbehalten.

Sachnummer: A31003-P3030-F100-32-0018

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 Software and Solutions GmbH & Co. KG. Alle anderen Marken-, Produkt- und Servicennamen sind Warenzeichen oder eingetragene Warenzeichen ihrer jeweiligen Inhaber.

atos.net

The logo for Atos, featuring the word "Atos" in a bold, white, sans-serif font. The letter 'o' is stylized with a circular cutout in the center.

Inhalt

1 Einführung und wichtige Hinweise.....	24
1.1 Über diese Dokumentation.....	24
1.1.1 Dokumentationen und Zielgruppen.....	25
1.1.2 Gliederung Administratordokumentation.....	26
1.1.3 Arten von Themen.....	29
1.1.4 Darstellungskonventionen.....	29
1.2 Sicherheits- und Warnhinweise.....	30
1.2.1 Warnhinweise: Gefahr.....	31
1.2.2 Warnhinweise: Warnung.....	31
1.2.3 Warnungen: Vorsicht.....	32
1.2.4 Warnhinweise: Hinweis.....	33
1.2.5 Länderspezifische Sicherheitshinweise.....	34
1.2.5.1 Sicherheitshinweise für Australien.....	34
1.2.5.2 Sicherheitshinweise für Brasilien.....	35
1.2.5.3 Sicherheitshinweise für USA.....	35
1.2.5.4 Sicherheitshinweise für Kanada.....	38
1.3 Wichtige Hinweise.....	39
1.3.1 Verhalten in Notfällen.....	39
1.3.2 Bestimmungsgemäßer Gebrauch.....	40
1.3.3 Sachgemäße Entsorgung und Recycling.....	40
1.3.4 Normen und Richtlinien bezüglich der Installation.....	41
1.3.4.1 Anschluss von OpenScape Office X an den Versorgungsstromkreis.....	41
1.3.4.2 Anschluss von OpenScape Business S und OpenScape Business UC Booster Server an den Versorgungsstromkreis.....	42
1.3.4.3 Geschirmte Verkabelung für LAN- und WAN-Anschlüsse von OpenScape Business X.....	42
1.3.4.4 Brandschutzanforderungen.....	43
1.3.4.5 Blitzschutzanforderungen.....	43
1.3.4.6 Kennzeichnungen für OpenScape Business X.....	44
1.3.5 Hinweise zu Störaussendung und Funkstörung von OpenScape Business X.....	44
1.3.6 Datenschutz und Datensicherheit.....	45
1.3.7 Technische Vorschriften und Konformität von OpenScape Business X.....	46
1.3.7.1 CE-Konformität.....	46
1.3.7.2 Konformität mit US- und kanadischen Normen.....	46
1.3.7.3 Konformität mit internationalen Normen.....	47
1.3.8 Betriebsbedingungen.....	47
1.3.8.1 Betriebsbedingungen OpenScape Business X.....	47
1.3.8.2 Betriebsbedingungen OpenScape Business S und OpenScape Business UC Booster Server.....	48
2 Systemübersicht.....	49
2.1 Highlights.....	49
2.2 Unified Communications.....	50
2.2.1 UC-Funktionen (Überblick).....	50
2.2.2 Benutzerzugriff auf UC-Funktionen (UC Clients).....	58
2.2.3 Integration in Geschäftsanwendungen.....	61
2.3 OpenScape Business Modelle.....	62
2.3.1 Vertriebliche Ausbaustufen.....	62
2.3.2 UC Hardware Modelle.....	66
2.3.3 UC Booster Hardware.....	67
2.3.4 UC Software Modelle (Softswitch).....	68

- 2.3.5 Aufbau und Umweltbedingungen..... 68
- 2.3.6 Unterstützte Telefone..... 69
- 2.4 Weiterführende Informationen..... 70
 - 2.4.1 Unterstützte Sprachen..... 70
 - 2.4.2 Internet-Links..... 72
- 3 Administrationskonzept..... 74**
- 3.1 OpenScape Business Assistant (WBM)..... 74
 - 3.1.1 Voraussetzungen für das WBM..... 74
 - 3.1.2 Startseite des WBM..... 74
 - 3.1.3 Einführung in das WBM..... 76
 - 3.1.4 Benutzerverwaltung des WBM..... 78
 - 3.1.5 Wizards..... 81
 - 3.1.5.1 Wizards – Grundinstallation..... 81
 - 3.1.5.2 Wizards – Netzwerk / Internet..... 82
 - 3.1.5.3 Wizards – Endgeräte / Teilnehmer..... 82
 - 3.1.5.4 Wizards – Zentrale Telefonie..... 83
 - 3.1.5.5 Wizards – User-Telefonie..... 83
 - 3.1.5.6 Wizards – Sicherheit..... 84
 - 3.1.5.7 Wizards – UC Smart (nur mit UC Smart)..... 85
 - 3.1.5.8 Wizards – UC Suite (nur mit UC Suite)..... 85
 - 3.1.5.9 Assistenten – Circuit..... 86
 - 3.1.5.10 Assistenten – Globales Verzeichnis..... 86
 - 3.1.6 Service-Center..... 86
 - 3.1.6.1 Service Center – **Dokumente**..... 86
 - 3.1.6.2 Service Center – **Software** 87
 - 3.1.6.3 Service Center – **Inventory > System**..... 87
 - 3.1.6.4 Service Center – **Inventory > Rufnummern**..... 87
 - 3.1.6.5 Service Center – **Inventory > Netzwerkübersicht**..... 87
 - 3.1.6.6 Service-Center – **Software-Update**..... 87
 - 3.1.6.7 Service-Center – **Email-Weiterleitung**..... 88
 - 3.1.6.8 Service-Center – **Remote-Zugang**..... 88
 - 3.1.6.9 Service-Center – **Restart / Reload**..... 88
 - 3.1.6.10 Service-Center – **Diagnose > Status**..... 88
 - 3.1.6.11 Service-Center – **Diagnose > Event Viewer**..... 88
 - 3.1.6.12 Service-Center – **Diagnose > Trace**..... 88
 - 3.1.6.13 Service-Center – Diagnose > Service-Protokoll..... 88
 - 3.1.7 Experten-Modus..... 89
 - 3.1.8 Online-Hilfe..... 89
- 3.2 Manager E..... 89
- 4 Ersteinrichtung von OpenScape Business X..... 91**
- 4.1 Voraussetzungen für die Erstinstallation..... 91
- 4.2 Komponenten..... 93
- 4.3 Rufnummernplan..... 94
- 4.4 IP-Adressen-Schema..... 95
- 4.5 Erstinbetriebnahme..... 97
- 4.6 Integration ins Kunden-LAN..... 97
 - 4.6.1 Systemeinstellungen..... 98
 - 4.6.2 DHCP-Einstellungen 98
 - 4.6.3 Länder- und Zeiteinstellungen..... 99
 - 4.6.4 UC-Lösung..... 100
 - 4.6.5 Anschluss des Kommunikationssystems ans Kunden-LAN..... 100
- 4.7 Basiskonfiguration..... 100
 - 4.7.1 Systemrufnummern und Vernetzung..... 101
 - 4.7.2 Teilnehmerdaten..... 101

4.7.3 ISDN-Konfiguration 103
 4.7.4 Internetzugang 103
 4.7.5 Internet-Telefonie 105
 4.7.6 Teilnehmer..... 106
 4.7.7 Konfiguration von UC Suite..... 107
 4.7.8 Konfiguration der UC Smart Sprachboxen..... 107
 4.7.9 Konferenz-Server-Einstellungen..... 107
 4.7.10 E-Mail-Versand (optional)..... 108
 4.8 Abschließende Tätigkeiten..... 108
 4.9 Inbetriebnahme der IP-Telefone..... 109

5 Ersteinrichtung von OpenScape Business S..... 111

5.1 Voraussetzungen für die Ersteinrichtung..... 111
 5.2 Komponenten..... 114
 5.3 IP-Adressen-Schema..... 115
 5.4 Rufnummernplan..... 116
 5.5 Installation der Kommunikationssoftware..... 116
 5.6 Inbetriebnahme..... 118
 5.6.1 Systemeinstellungen..... 118
 5.6.2 UC-Lösung..... 119
 5.7 Basiskonfiguration..... 119
 5.7.1 Systemrufnummern und Vernetzung..... 119
 5.7.2 Teilnehmerdaten..... 120
 5.7.3 Internet-Telefonie 121
 5.7.4 Teilnehmer..... 122
 5.7.5 Konfiguration von UC Suite..... 123
 5.7.6 Konfiguration der UC Smart Sprachboxen..... 123
 5.7.7 Konferenz-Server-Einstellungen..... 123
 5.7.8 E-Mail-Versand (optional)..... 123
 5.8 Abschließende Tätigkeiten..... 124
 5.9 Inbetriebnahme der IP-Telefone..... 124
 5.10 Deinstallation der Kommunikationssoftware..... 126
 5.11 Verwendete Ports..... 126

6 Ersteinrichtung OpenScape Business UC Booster..... 129

6.1 Voraussetzungen für die Ersteinrichtung..... 132
 6.2 Sicherung der Konfigurationsdaten des Kommunikationssystems..... 134
 6.2.1 Wie Sie eine Datensicherung durchführen..... 135
 6.3 Inbetriebnahme UC Booster Card..... 135
 6.3.1 Montage der UC Booster Card..... 135
 6.3.2 Konfiguration der UC Booster Card..... 136
 6.3.3 Software-Update für die UC Booster Card..... 136
 6.3.3.1 Wie Sie ein Software-Update durchführen..... 137
 6.4 Inbetriebnahme UC Booster Server..... 137
 6.4.1 Installation der Kommunikationssoftware..... 137
 6.4.1.1 Wie Sie die Kommunikationssoftware installieren..... 139
 6.4.2 Konfiguration des UC Booster Servers..... 141
 6.4.2.1 IP-Adresse des Kommunikationssystems bekannt geben..... 141
 6.4.3 Software-Update für die UC Booster Server..... 143
 6.5 Basiskonfiguration..... 144
 6.6 Abschließende Tätigkeiten..... 144
 6.7 Deinstallation der Kommunikationssoftware..... 145
 6.7.1 Wie Sie die Kommunikationssoftware deinstallieren..... 145
 6.8 Hochrüstung von UC Booster Card auf UC Booster Server..... 145
 6.9 Verwendete Ports..... 147

7 Lizenzierung..... 150

- 7.1 Lizenzierungsverfahren..... 151
- 7.2 Lizenzen..... 153
 - 7.2.1 Basislizenz..... 155
 - 7.2.2 Benutzerlizenzen..... 155
 - 7.2.3 User-orientierte Lizenzen..... 157
 - 7.2.4 Systemlizenzen..... 158
 - 7.2.5 Evaluierungslizenzen..... 161
 - 7.2.6 Upgrade-Lizenzen..... 163
 - 7.2.7 Vorschläge für Lizenzkombinationen..... 164
- 7.3 Lizenzierung eines Kommunikationssystems (Standalone)..... 166
 - 7.3.1 CLS Connect..... 167
 - 7.3.2 Lizenzaktivierung (Standalone) 167
 - 7.3.3 Lizenzzuordnung (Standalone)..... 168
- 7.4 Lizenzierung mehrerer Kommunikationssysteme (Netzverbund)..... 171
 - 7.4.1 Lizenzaktivierung (Netzverbund)..... 173
 - 7.4.2 Lizenzzuordnung (Netzverbund)..... 174
- 7.5 Lizenzinformationen..... 177
 - 7.5.1 Lizenzinformationen ohne Netzverbund (Standalone)..... 178
 - 7.5.2 Lizenzinformationen im Netzverbund 178
- 7.6 Lizenzprofilzuordnung 178
- 7.7 Rehost nach Hardwaretausch..... 179
- 7.8 Lizenzserver (Central License Server, CLS) 179
- 7.9 Lizenzagent (Customer License Agent, CLA)..... 180
- 7.10 Locking ID und Advanced Locking ID..... 180
- 8 Integration ins interne Datennetz (LAN)..... 183**
 - 8.1 LAN-Schnittstelle..... 183
 - 8.1.1 IP-Adresse und Netzmaske der LAN-Schnittstelle..... 183
 - 8.1.2 Interner IP-Adressbereich der LAN-Schnittstelle..... 184
 - 8.2 DHCP..... 184
 - 8.2.1 DHCP-Relay-Agent..... 185
 - 8.2.2 DHCP-Server 185
 - 8.3 DNS - Namensauflösung..... 186
 - 8.4 IP-Routing..... 188
 - 8.5 Deployment Service (DLI und DLS)..... 188
- 9 Anbindung an Service-Provider..... 192**
 - 9.1 Internetzugang..... 192
 - 9.1.1 Internet-Zugang über einen externen Internet-Router 194
 - 9.1.2 Internet-Zugang über Internet-Modem 195
 - 9.1.3 WAN-Schnittstelle..... 196
 - 9.1.4 DynDNS..... 196
 - 9.2 Amtszugang über ITSP..... 197
 - 9.2.1 Konfiguration eines ITSP..... 199
 - 9.2.2 STUN (Simple Traversal of UDP over NAT)..... 201
 - 9.3 Amtszugang über digitale und analoge Leitungen..... 202
 - 9.3.1 Leitungen..... 202
 - 9.3.2 Richtungen..... 203
 - 9.3.3 Wähltonüberwachung..... 206
 - 9.4 Priorisierung der Amtsholung bei aktiviertem LCR..... 208
- 10 Teilnehmer..... 209**
 - 10.1 Rufnummernplan..... 209
 - 10.1.1 Standard-Rufnummernplan..... 210
 - 10.1.2 Individueller Rufnummernplan..... 211
 - 10.2 Anforderungen an die LAN-Telefonie..... 212
 - 10.2.1 Audio-Codex..... 212

10.2.2 Übertragung von Tönen nach RFC2833.....	214
10.2.3 Quality of Service.....	214
10.3 IP-Teilnehmer.....	216
10.4 SIP-Teilnehmer.....	217
10.5 UP0-Teilnehmer.....	219
10.6 DECT-Teilnehmer.....	220
10.7 ISDN-Teilnehmer.....	221
10.8 Analoge Teilnehmer.....	222
10.9 Virtuelle Teilnehmer.....	224
10.10 Tastenprogrammierung	224
10.11 Teilnehmer-Profile.....	225
10.12 Konfiguration der Teilnehmer.....	225
10.13 Konfiguration der Teilnehmer-Profile	228
10.14 Konfiguration der Authentifizierungsdaten am SIP-Telefon.....	228
10.15 Export von Teilnehmerdaten.....	229
11 UC Smart.....	230
11.1 Grundeinstellungen für UC Smart.....	231
11.2 UC Smart Clients.....	232
11.2.1 myPortal @work.....	232
11.2.1.1 Voraussetzungen für myPortal @work.....	234
11.2.1.2 myPortal@work: Benutzerkonfiguration.....	236
11.2.1.3 Konfigurationsschritte zur Nutzung von myPortal @work über das Internet.....	243
11.2.1.4 Weitere Konfigurationshinweise & Einstellungen.....	245
11.2.1.5 Leitfaden zur Fehlerbehebung.....	247
11.2.1.6 Weitere Hinweise.....	249
11.3 Benutzer von UC Smart.....	250
11.4 Anwesenheitsstatus (Präsenz).....	251
11.5 Verzeichnisse und Journal.....	252
11.5.1 Verzeichnisse.....	252
11.5.2 Internes Verzeichnis.....	253
11.5.3 Favoritenliste.....	253
11.5.4 Systemverzeichnis.....	253
11.5.5 Unified-Verzeichnis.....	253
11.5.5.1 Leistungsmerkmale.....	254
11.5.5.2 Regeln und Konventionen.....	258
11.5.5.3 Funktionale Grenzen.....	259
11.5.5.4 Unified-Verzeichnis in vernetzten Systemen.....	259
11.5.6 Journal.....	260
11.6 Anrufe.....	261
11.6.1 Rufnummernformate.....	261
11.6.2 Voraussetzungen für den Empfang von VoIP-Anrufen auf myPortal to go mit CallKit auf Ihrem iPhone.....	262
11.7 Konferenzen.....	262
11.8 Web Collaboration.....	264
11.9 Instant Messaging.....	265
11.9.1 Instant Messaging.....	265
11.10 Sprachbox (SmartVM).....	265
11.10.1 Konfiguration der Sprachbox (SmartVM)	268
11.10.2 Benachrichtigungsdienst für neue Nachrichten.....	269
12 UC Suite.....	270
12.1 Grundeinstellungen für UC Suite.....	270
12.2 UC Suite Clients.....	271
12.2.1 myPortal for Desktop.....	271
12.2.2 myPortal @work.....	272

Inhalt

12.2.3 myPortal for Outlook.....	272
12.2.4 Fax Printer.....	272
12.2.5 myAttendant.....	273
12.2.6 Voraussetzungen für UC Suite PC-Clients.....	273
12.2.7 Silent Installation/Deinstallation für UC Suite PC-Clients.....	277
12.2.8 Automatische Updates.....	279
12.3 Benutzer und Benutzer-Profile von UC Suite.....	279
12.3.1 Benutzer von UC Suite.....	279
12.3.2 Benutzer-Profile der UC Suite.....	282
12.4 Anwesenheitsstatus und CallMe-Dienst.....	284
12.4.1 Anwesenheitsstatus (Präsenz).....	284
12.4.2 CallMe-Dienst.....	287
12.4.3 Statusbezogene Anrufumleitung.....	288
12.4.4 Regelbasierte Anrufumleitung.....	289
12.5 Verzeichnisse und Journal.....	290
12.5.1 Verzeichnisse.....	290
12.5.2 Internes Verzeichnis.....	293
12.5.3 Externes Verzeichnis.....	293
12.5.4 Externes Offline-Verzeichnis (LDAP).....	294
12.5.5 Systemverzeichnis.....	295
12.5.6 Unified-Verzeichnis.....	295
12.5.6.1 Leistungsmerkmale.....	296
12.5.6.2 Regeln und Konventionen.....	300
12.5.6.3 Funktionale Grenzen.....	301
12.5.6.4 Unified-Verzeichnis in vernetzten Systemen.....	301
12.5.7 Abteilungen.....	302
12.5.8 Favoritenliste.....	302
12.5.9 Journal.....	303
12.6 Anrufe.....	305
12.6.1 Desktop-Wahl und Clipboard-Wahl.....	305
12.6.2 PopUp-Fenster.....	305
12.6.3 Aufzeichnen von Anrufen.....	306
12.7 Konferenzen.....	306
12.7.1 Konferenzmanagement.....	306
12.7.2 Ad-hoc-Konferenz.....	310
12.7.3 Geplante Konferenz.....	311
12.7.4 Permanente Konferenz.....	313
12.7.5 Offene Konferenz.....	314
12.8 Web Collaboration.....	315
12.9 Instant Messaging.....	316
12.9.1 Sofortnachricht versenden.....	316
12.10 AutoAttendant.....	317
12.10.1 Persönlicher AutoAttendant.....	318
12.11 Sprach- und Faxnachrichten.....	318
12.11.1 Voicemail-Postfach.....	318
12.11.2 Ansagen der Sprachbox.....	320
12.11.3 Faxbox.....	322
12.11.4 Senden von Faxnachrichten mit Fax Printer.....	323
12.11.5 Benachrichtigungsdienst für neue Nachrichten (UC Suite).....	324
12.11.6 E-Mail-Versand.....	325
12.11.7 SMS-Template.....	325
12.11.8 Fax over IP (T.38 / G.711-Fax).....	326
12.12 Überblick über Integration von Microsoft Office 365.....	327
13 Funktionen am Telefon.....	328
13.1 Anrufen.....	328

- 13.1.1 Ziffernwahl..... 328
- 13.1.2 Blockwahl..... 328
- 13.1.3 Keypad-Wahl..... 328
- 13.1.4 Wahlendeerkennung..... 329
- 13.1.5 Editieren der Wahl..... 329
- 13.1.6 Wahlwiederholung..... 330
- 13.1.7 Kurzwahl zentral KWZ..... 331
- 13.1.8 Kurzwahl individuell (KWI)..... 332
- 13.1.9 Direktruf..... 333
- 13.1.10 Direktansprechen / Direktantworten..... 333
- 13.1.11 Assoziierte Wahl..... 334
- 13.1.12 Leitungsvormerken..... 335
- 13.1.13 Privatleitung..... 335
- 13.2 Anrufsignalisierung, Rufnummernanzeige..... 336
 - 13.2.1 Unterschiedliche Anrufsignalisierung..... 336
 - 13.2.2 Calling Line Identification Presentation (CLIP)..... 336
 - 13.2.3 Calling Line Identification Restriction (CLIR)..... 337
 - 13.2.4 Rufnummernübermittlung des Angerufenen (COLP)..... 338
 - 13.2.5 Rufnummernunterdrückung des Angerufenen (COLR)..... 338
 - 13.2.6 CLIP no screening (Übermittlung kundenspezifischer Rufnummerninformationen)..... 338
 - 13.2.7 CLIP für analoge Endgeräte..... 339
 - 13.2.8 Stillter Ruf / Ruhe..... 339
 - 13.2.9 Rufnummernumwertung in Namen bei Kurzwahl zentral..... 340
- 13.3 Funktionen während der Verbindung..... 340
 - 13.3.1 Halten..... 340
 - 13.3.2 Parken..... 340
 - 13.3.3 Rückfrage..... 341
 - 13.3.4 Makeln..... 342
 - 13.3.5 Übergabe..... 342
 - 13.3.6 Wiederanruf..... 343
 - 13.3.7 Call Supervisor..... 344
 - 13.3.8 Diskretes Ansprechen..... 345
 - 13.3.9 Live Call Recording (Voice Recording; Sprachaufzeichnung)..... 346
- 13.4 Steuern der Erreichbarkeit..... 348
 - 13.4.1 Anrufumleitung 348
 - 13.4.2 Anrufumleitung (CF)..... 349
 - 13.4.3 Anrufumleitung nach Zeit..... 351
 - 13.4.4 Rufweitschaltung im Amt (nicht für USA)..... 352
 - 13.4.5 Rufzuordnung..... 352
 - 13.4.6 Rufzuschaltung..... 353
 - 13.4.7 Anrufe abweisen..... 354
 - 13.4.8 Zurückstellen eines Anrufs..... 354
 - 13.4.9 Anrufschutz..... 355
- 13.5 Optimieren der Kommunikationsabläufe..... 356
 - 13.5.1 Rückruf..... 356
 - 13.5.2 Anklopfen..... 357
 - 13.5.3 Aufschalten..... 358
 - 13.5.4 Abwesenheitstexte..... 359
 - 13.5.5 Mitteilungstexte..... 359
 - 13.5.6 Assoziierte Dienste..... 360
 - 13.5.7 DISA..... 360
 - 13.5.8 Flex Call/Mobile PIN..... 361
 - 13.5.9 Relocate/Rufnummerntausch..... 362
 - 13.5.10 Rücksetzen aktivierter Leistungsmerkmale..... 363
 - 13.5.11 Prozeduren..... 363
 - 13.5.12 Weckeinrichtung und Termine..... 365

13.6 Übersicht über Funktionen und Codes..... 365

14 Arbeiten im Team (Gruppen)..... 370

14.1 Anrufübernahmegruppe, Gruppenruf und Sammelanschluss..... 370

 14.1.1 Anrufübernahmegruppe 370

 14.1.2 Gruppenruf..... 372

 14.1.3 Sammelanschluss..... 377

 14.1.4 Konfiguration von Anrufübernahmegruppen, Gruppenrufen und Sammelanschlüssen über Wizards 380

 14.1.5 Konfiguration von Anrufübernahmegruppen, Gruppenrufen und Sammelanschlüssen über Experten-Modus..... 381

14.2 Teamschaltung / Team-Gruppe und Chef/Sekretär / Top-Gruppe..... 381

 14.2.1 Teamschaltung / Team-Gruppe..... 382

 14.2.2 Chef/Sekretär / Top-Gruppe..... 386

 14.2.3 Konfiguration von Teamschaltungen / Team-Gruppen und Chef/Sekretär-Funktionen / Top-Gruppen über Wizards 390

 14.2.4 Konfiguration von Teamschaltungen / Team-Gruppen und Chef/Sekretär-Funktionen / Top-Gruppen über Experten-Modus..... 391

14.3 Basic-MULAP und Chef-MULAP..... 391

 14.3.1 Basic-MULAP..... 392

 14.3.2 Chef-MULAP..... 394

 14.3.3 Konfiguration von Basic-MULAPs und Chef-MULAPs..... 397

14.4 Sprachbox-Gruppe und Faxbox-Gruppe..... 397

 14.4.1 Sprachbox-Gruppe..... 398

 14.4.2 Faxbox-Gruppe..... 398

 14.4.3 Konfiguration von Sprachbox-Gruppen und Faxbox-Gruppen..... 399

14.5 Direktansprechen für Gruppen..... 399

 14.5.1 Durchsage an Gruppe..... 399

 14.5.2 Übergabe an Gruppe aus Durchsage..... 400

14.6 Anrufverteilung (UCD Uniform Call Distribution)..... 400

 14.6.1 Anrufverteilung / UCD-Gruppe..... 401

 14.6.2 UCD-Agenten..... 402

 14.6.3 Nachbearbeitung..... 404

 14.6.4 Priorisierte Anrufordnung..... 404

 14.6.5 UCD-Anrufe automatisch annehmen..... 405

 14.6.6 UCD-Warteschlange..... 405

 14.6.7 UCD-Überlauf..... 406

 14.6.8 UCD-Nachtschaltung..... 407

 14.6.9 Ansagen / Wartemusik bei UCD..... 408

 14.6.10 Übergabe an UCD-Gruppen..... 408

 14.6.11 Auslösen von UCD-Anrufen über analoge Leitungen..... 409

15 Anruf-Routing..... 410

15.1 Berechtigungen (Wahlkontrolle)..... 410

 15.1.1 Berechtigungsgruppen und Berechtigungsklassen..... 410

 15.1.2 Erlaubnis- und Verbotslisten..... 411

 15.1.3 Blacklist..... 412

 15.1.4 Nachtschaltung..... 413

 15.1.5 Automatische Berechtigungsumschaltung nach Zeit..... 414

 15.1.5.1 Zeitplan..... 415

 15.1.6 VBZ (Verkehrsbeziehungen)..... 416

 15.1.6.1 VBZ-Gruppen (Verkehrsbeziehungsgruppen)..... 417

 15.1.6.2 Zuordnung der KWZ-Nummern zu VBZ-Gruppen..... 417

 15.1.7 Zentrales Codeschloss, Berechtigungsumschaltung..... 418

 15.1.8 Individuelles Codeschloss (Telefon abschließen)..... 418

 15.1.9 R-Gesprächsschutz je Amtsleitung (nur für Brasilien)..... 419

- 15.1.10 R-Gesprächsschutz je Teilnehmer (nur für Brasilien)..... 419
- 15.2 LCR (Least Cost Routing, Leitweglenkung)..... 419
 - 15.2.1 LCR-Funktionalität..... 420
 - 15.2.2 LCR-Wahlplan..... 422
 - 15.2.3 LCR-Wegetabelle..... 424
 - 15.2.4 LCR-Berechtigung..... 425
 - 15.2.5 LCR-Wahlregeln..... 425
 - 15.2.6 Netzanbieter..... 427
 - 15.2.7 Gezielte Belegung von Amtsleitungen..... 428
- 15.3 Wahlbewertung und Call-Routing..... 429
 - 15.3.1 Überblick Call Routing / LCR..... 430
 - 15.3.2 Flußdiagramm Wahlbewertung..... 432
 - 15.3.3 Call Routing und LCR im Netzverbund..... 433
 - 15.3.3.1 Dediziertes Gateway..... 435
 - 15.3.4 Szenarien: Wahlbewertung und Call Routing..... 436
 - 15.3.4.1 Teilnehmer A ruft Teilnehmer B über Internrufnummer..... 437
 - 15.3.4.2 Teilnehmer A ruft Teilnehmer B über öffentliche Rufnummer..... 437
 - 15.3.4.3 Teilnehmer A ruft externen Teilnehmer über Amt..... 439
 - 15.3.4.4 ISDN-Amt ruft Teilnehmer A..... 440
 - 15.3.4.5 Sonderkonfigurationen..... 440
 - 15.3.4.6 Teilnehmer A ruft Teilnehmer C über Internrufnummer..... 441
 - 15.3.4.7 Teilnehmer A ruft Teilnehmer C über öffentliche Rufnummer im Netzverbund..... 443
 - 15.3.4.8 ISDN-Amt ruft Teilnehmer C..... 446
 - 15.3.4.9 ISDN-Amt Gateway 1 ruft Teilnehmer D..... 447
 - 15.3.4.10 Teilnehmer D ruft externen Teilnehmer über Amt..... 450
- 15.4 Notrufe..... 452
 - 15.4.1 Röchelschaltung / Hotline..... 453
 - 15.4.2 Leitungstrennung für einen Notruf..... 454
 - 15.4.3 Nur für USA, Kanada: Notrufdienst E911..... 454
 - 15.4.4 Notrufe in Kombination mit Mobile Logon..... 455
 - 15.4.4.1 Konfiguration des Notrufszenarios..... 455
 - 15.4.5 Notrufdienst E112 (für Europa)..... 458
- 15.5 Anrufsteuerungsdienst (Call Admission Control)..... 458
 - 15.5.1 Einschränkung der Anzahl gleichzeitiger Gespräche über ITSP..... 459
 - 15.5.2 Einschränkung des Bandbreitenbedarfs bei Gateway-Gesprächen..... 459
 - 15.5.3 Einschränkung der Anzahl der Gespräche in Vernetzungsszenarien..... 459
- 15.6 Gemeinschaftsanlage..... 460
 - 15.6.1 Kurzwahl zentral in Gemeinschaftsanlagen..... 461
- 16 Attendants..... 463**
 - 16.1 AutoAttendant..... 463
 - 16.1.1 Company AutoAttendant (UC Smart)..... 465
 - 16.1.2 Company AutoAttendant (UC Suite)..... 466
 - 16.1.2.1 Zeitpläne..... 466
 - 16.1.2.2 Vorlagen (Templates)..... 474
 - 16.1.3 Xpressions Compact..... 476
 - 16.2 OpenStage Attendant..... 477
 - 16.3 OpenScape Business Attendant..... 477
 - 16.3.1 OpenScape Business BLF..... 480
 - 16.3.2 Einrichtebeispiele für OpenScape Business Attendant, OpenScape Business BLF..... 481
 - 16.4 myAttendant..... 481
 - 16.4.1 Teilnehmerverwaltung..... 483
 - 16.4.2 Nachrichtencenter 483
 - 16.5 Abwurfplatz..... 484
- 17 Multimedia Contact Center..... 487**

17.1	Contact Center Clients.....	487
17.1.1	myAgent.....	488
17.1.2	Voraussetzungen für myAgent.....	489
17.1.3	myReports.....	491
17.1.4	Voraussetzungen für myReports.....	493
17.1.5	Hinweise zur gleichzeitigen Nutzung von myAgent und UC Suite Clients.....	495
17.2	Agenten.....	496
17.2.1	Berechtigungsabhängige Funktionen für Agenten.....	496
17.2.2	Bevorzugte Agenten.....	498
17.2.3	Agent in mehreren Warteschlangen.....	498
17.2.4	Contact Center Pausen.....	498
17.2.5	An- und Abmeldung des Agenten per Telefon.....	498
17.3	Warteschlangen und Zeitpläne.....	502
17.3.1	Warteschlangen.....	502
17.3.2	Zeitpläne.....	504
17.3.3	Nachbearbeitung.....	513
17.3.4	Servicegrad.....	514
17.3.5	Wandanzeige (Wallboard).....	514
17.3.6	Agentenrückruf.....	515
17.4	VIP-Betreuung.....	515
17.4.1	VIP-Anruferpriorität.....	515
17.4.2	VIP-Rufliste.....	515
17.5	Rückfalllösung (Fallback-Lösung).....	516
17.6	Konfiguration des Contact Centers.....	520
17.6.1	Beispiel für eine Contact-Center-Konfiguration.....	520
17.6.2	Vorgehensweise bei der Konfiguration.....	522
17.7	Hinweise zum Einsatz des Contact Centers.....	523
17.7.1	Einschränkungen beim Betrieb des Contact Centers.....	523
17.8	Hinweise zum Einsatz von DECT-Telefonen.....	526
17.9	Berichte.....	527
17.9.1	Vordefinierte Berichtsvorlagen.....	528
18	Mobility.....	530
18.1	Integrierte Mobilitätslösungen.....	530
18.2	Mobilität unterwegs.....	530
18.2.1	myPortal to go.....	531
18.2.1.1	Voraussetzungen: myPortal to go.....	533
18.2.2	Mobility Entry.....	535
18.2.3	Vergleich Mobile Clients und Mobility Entry.....	537
18.2.4	Abhängigkeiten für Mobile Clients und Mobility Entry.....	538
18.2.5	One Number Service.....	540
18.2.6	Dual-Mode-Telefonie.....	540
18.2.7	Konfiguration von myPortal to go und Mobility Entry	541
18.3	Mobilität im Büro.....	542
18.3.1	DeskSharing.....	542
18.3.2	Integrierte Cordless-Lösung.....	544
18.3.2.1	Systemübersicht.....	545
18.3.2.2	Cordless-Baugruppenanschaltung.....	546
18.3.2.3	Systemausbau.....	546
18.3.2.4	Cordless/DECT-Telefone.....	548
18.3.2.5	Bedeutung der Ergebnisse beim Test des Funkbereichs.....	548
18.3.3	Konfiguration der integrierten Cordless-Lösung.....	551
18.3.4	Cordless IP.....	552
18.3.5	WLAN-Telefone und Access Points.....	552
18.3.5.1	Anforderungen an das WLAN.....	552
18.4	Mobilität zu Hause.....	552

18.4.1 Konfiguration für VPN..... 554

18.4.2 Konfiguration für SIP-Gerät@Home..... 554

18.4.3 Konfiguration für Systemgerät@Home..... 556

19 Sicherheit..... 559

19.1 Firewall..... 559

 19.1.1 Porthandling..... 559

 19.1.1.1 Portfreigabe..... 560

 19.1.1.2 Port-Verwaltung..... 561

 19.1.2 NAT..... 561

 19.1.3 Application Firewall..... 562

 19.1.4 Dienstverwaltung (OpenScape Business S)..... 563

19.2 Signaling- und Payload-Encryption (SPE)..... 563

19.3 Virtual Private Network VPN 565

 19.3.1 Anforderungen für VPN..... 566

 19.3.2 Anbindung von Teleworkern über VPN..... 568

 19.3.3 Vernetzung von Kommunikationssystemen über VPN..... 569

 19.3.4 VPN - Sicherheitsmechanismen..... 570

 19.3.5 VPN - Zertifikate..... 572

 19.3.6 VPN-Clients..... 574

 19.3.6.1 NCP VPN Client Einstellungen..... 575

 19.3.7 VPN - Dienste..... 577

 19.3.8 VPN-Tunnel..... 577

 19.3.9 VPN-Regeln..... 577

 19.3.10 PKI-Server..... 578

19.4 Zertifikatshandling..... 578

19.5 Web Sicherheit..... 579

 19.5.1 Verbindungen zum Web-Server..... 579

 19.5.2 Admin-Protokoll..... 579

19.6 SQL-Sicherheit..... 579

 19.6.1 Einzelknoten..... 580

 19.6.2 Mehrfachknoten..... 580

19.7 Schutz vor SIP-Attacken (SIP Attack Protection)..... 581

20 Vernetzung von OpenScape Business..... 583

20.1 Vernetzungsplan..... 584

 20.1.1 Homogene und inhomogene Netze 584

 20.1.2 Single- und Multi-Gateway..... 585

20.2 Netzweite Leistungsmerkmale..... 586

 20.2.1 Netzweite Leistungsmerkmale der UC-Lösungen..... 586

 20.2.2 Netzweite Voice-Leistungsmerkmale..... 589

20.3 Lizenzierung eines Netzverbundes..... 590

20.4 Anforderungen an die Vernetzung..... 590

 20.4.1 Anforderungen an die LAN-Vernetzung..... 591

 20.4.2 Rufnummernplan im Netz..... 593

 20.4.2.1 Wahl von öffentlichen Rufnummern im Netz..... 594

20.5 Wegeoptimierung (Path Replacement)..... 594

20.6 Vernetzungsszenarien..... 595

 20.6.1 Abhängigkeiten und Einschränkungen..... 596

 20.6.2 Vernetzung von mehreren OpenScape Business X..... 597

 20.6.3 Vernetzung von OpenScape Business X mit OpenScape Business S (Single Gateway)..... 601

 20.6.4 Vernetzung von Open Scape Business X und OpenScape Business S (Multi Gateway)..... 608

 20.6.5 Vernetzung von OpenScape Business in Hosting-Umgebungen..... 616

 20.6.6 Vernetzung von OpenScape Business X und OpenScape 4000..... 619

20.6.7 Vernetzung von OpenScape Business X und OpenScape Voice.....	627
20.6.8 Anbindung von externen Anschaltungen an OpenScape Business über SIP- Interconnection.....	630
20.6.9 Offene Nummerierung in OpenScape Business X Netzwerken.....	632
20.6.9.1 Wie Sie die offene Nummerierung konfigurieren.....	633
20.6.10 Vernetzung über ISDN.....	634
20.6.11 OpenScape Business Netzverbund mit zentralem ITSP-Amtsanschluss.....	636
20.7 Zentraler Abwurfplatz im Netzverbund (nicht für USA).....	638
20.8 Presence Manager.....	639
20.9 Synchronisationsstatus im Netzverbund.....	639
20.9.1 Manuelle Synchronisierung im Netzverbund.....	640
20.10 Survivability.....	641
20.11 Entfernung eines Knotens aus dem Netzverbund.....	643
21 Anschaltungen.....	644
21.1 Analoges Ansagegerät.....	644
21.2 Türsprechstelle und Türöffner.....	645
21.2.1 DoorLine a/b T01-T04.....	645
21.2.2 DoorCom Analog.....	646
21.2.3 Türfreisprecheinrichtung mit Verstärker (TFE-S).....	647
21.2.4 Lautsprecher.....	649
21.3 Aktoren.....	650
21.4 Sensoren.....	652
21.5 OpenStage Gate View.....	653
21.5.1 Rechtliche Rahmenbedingungen.....	654
21.5.2 Komponenten.....	654
21.5.3 Funktionsübersicht.....	655
21.5.4 Menü.....	656
21.5.5 OpenStage Gate View Ersteinrichtung.....	657
21.5.6 OpenStage Gate View Videoaufzeichnung.....	658
21.5.7 OpenStage Gate View Türsprechstelle.....	659
21.5.8 OpenStage Gate View Benutzerverwaltung.....	659
21.5.9 OpenStage Gate View Server-Administration.....	660
21.5.10 OpenStage Gate View Anpassungen.....	660
22 Application Connectivity.....	661
22.1 CSTA.....	661
22.2 OpenScape Business TAPI 120/170.....	664
22.2.1 OpenScape Business TAPI 120.....	665
22.2.2 OpenScape Business TAPI 170.....	670
22.3 Web Services Interface.....	674
22.4 Open Directory Service.....	675
22.5 Active Directory Integration Service.....	679
22.6 Application Launcher.....	681
22.6.1 Voraussetzungen für Application Launcher.....	681
22.6.2 Profil mit Konfigurationsdaten von Application Launcher.....	682
22.7 Circuit.....	683
22.8 myPortal for Teams im Überblick.....	683
22.9 Unify Phone.....	684
23 Accounting.....	685
23.1 Verbindungsdaten.....	685
23.1.1 Erfassung von Verbindungsdaten.....	685
23.1.2 Projektkennzahlen.....	686
23.2 Anzeige und Übertragung von Verbindungsdaten.....	687
23.2.1 Übermittlung von Geldbeträgen (nicht für USA).....	687
23.2.2 Anzeige der Verbindungskosten am Telefon.....	688

23.2.3 Anzeige der Verbindungsdauer am Telefon..... 689

23.2.4 Übertragung von Verbindungsdaten.....689

23.3 Kostenkontrolle..... 697

23.3.1 Hinweis auf teure Verbindungswege..... 697

23.3.2 Schutz vor Gebührenbetrug..... 697

23.4 Accounting-Tools..... 697

23.4.1 Accounting Manager..... 698

23.4.2 Teledata Office..... 698

24 Wartung..... 699

24.1 Telefonie-Konfiguration..... 699

24.1.1 Datum und Uhrzeit..... 699

24.1.2 SNTP..... 700

24.1.3 Telefon-Logos..... 700

24.1.4 Kundenindividuelle Displayanzeige.....700

24.1.5 Mehrsprachige Textausgabe.....701

24.1.6 Flexible Menüs.....701

24.1.7 Wartemusik..... 701

24.1.8 Ansagen..... 703

24.1.9 Teilnehmer-zu-Teilnehmer Zeichengabe.....704

24.1.10 Sprachkanal-Signalisierungsschutz.....704

24.1.11 Zeitparameter..... 704

24.1.12 Steuerung von Centrex-Leistungsmerkmalen..... 704

24.2 Sichern und Wiederherstellen..... 705

24.2.1 Backup-Sets 706

24.2.2 Backup-Medien 706

24.2.3 Sofortiges Sichern 707

24.2.4 Zeitgesteuertes Sichern 708

24.2.5 Wiederherstellen 708

24.3 Updates..... 708

24.3.1 Nutzung eines lokalen Webservers..... 710

24.3.2 Update des Kommunikationssystems 711

24.3.3 Update der Systemtelefone..... 712

24.3.4 Software-Status..... 713

24.4 Restart, Reload, Shutdown..... 713

24.4.1 Restart (Neustart) von OpenScape Business..... 713

24.4.2 Reload von OpenScape Business..... 714

24.4.3 Shutdown (Herunterfahren) von OpenScape Business X..... 715

24.4.4 PIN für das kontrollierte Herunterfahren (Shutdown) von OpenScape Business X..... 715

24.4.5 Restart (Neustart) der UC Booster Card (Application Board OCAB)..... 715

24.4.6 Reload der UC Booster Card (Application Board OCAB)..... 715

24.4.7 Restart (Neustart) der UC Applikation..... 716

24.5 Inventory-Management..... 716

24.5.1 Systemstatus 716

24.5.2 Inventory 717

24.6 Automatische Aktionen..... 718

24.6.1 Automatische Aktion Garbage Collection..... 719

24.6.2 Automatische Aktion DLS Notification..... 719

24.6.3 Warnmechanismus für SDHC-Kartenlebensdauer..... 719

24.7 Power Management..... 721

24.8 Überwachung und Wartung von OpenScape Business..... 722

24.8.1 Prüfen einer Netzwerkverbindung von OpenScape Business X..... 722

24.8.2 SNMP (Simple Network Management Protocol)..... 722

24.8.3 Manuelle Aktionen..... 736

24.8.4 Traces 738

24.9 TCP-Dump..... 746

24.10 RPCAP-Dämon..... 746

24.11 Ereignisse.....747

24.12 Konfigurationsdaten für die Diagnose..... 749

24.13 Card Manager..... 750

24.14 Überwachung und Wartung der UC Suite..... 750

 24.14.1 Protokollierung..... 750

 24.14.2 Benachrichtigung..... 752

 24.14.3 Wartung..... 754

24.15 Überwachung der UC Smart..... 755

24.16 Remote Services..... 756

 24.16.1 RSP.servicelink..... 756

 24.16.2 Remote-Zugang..... 759

 24.16.3 Online-Benutzer..... 760

25 Migration..... 761

25.1 Software-Aktualisierung für OpenScape Business X Systeme..... 762

 25.1.1 Software-Aktualisierung von OpenScape Business X V2 auf OpenScape Business X V3..... 763

 25.1.2 Software-Aktualisierung von OpenScape Business X V1 auf V2..... 764

25.2 Software-Aktualisierung von UC Booster Server auf OpenScape Business X V3..... 765

 25.2.1 Wie Sie UC Business Booster Server V2 auf V3 aktualisieren..... 765

 25.2.2 Wie Sie UC Business Booster Server V1 auf V2 aktualisieren..... 767

25.3 Hardware/Software-Migration von OpenScape Business X Systemen auf V3..... 768

 25.3.1 Migration von OpenScape Business X V2 auf OpenScape Business X V3..... 769

 25.3.1.1 Wie Sie permanent lizenzierte Systeme mit CLS Connect auf V3 migrieren..... 770

 25.3.1.2 Wie Sie permanent lizenzierte Systeme ohne CLS Connect auf V3 migrieren..... 771

 25.3.1.3 Wie Sie PayGo-lizenzierte Systeme auf V3 migrieren..... 772

 25.3.2 Migration von OpenScape Business X V1 auf OpenScape Business X V3..... 773

 25.3.2.1 Schritt 1: Software-Aktualisierung von Version V1R3 auf zuletzt veröffentlichte Version V2R7..... 774

 25.3.2.2 Schritt 2: Migration des V2-Systems auf das V3-System..... 774

25.4 OpenScape Business X V3 System von einem V2-Mainboard auf ein V3-Mainboard migrieren..... 774

 25.4.1 Wie Sie permanent lizenzierte Systeme mit CLS Connect auf ein V3-Mainboard migrieren..... 776

 25.4.2 Wie Sie permanent lizenzierte Systeme ohne CLS Connect auf ein V3-Mainboard migrieren..... 777

 25.4.3 Wie Sie PayGo-lizenzierte Systeme auf ein V3-Mainboard migrieren..... 778

25.5 Software-Aktualisierung von OpenScape Business S..... 779

 25.5.1 Software-Aktualisierung von OpenScape Business S V2 auf OpenScape Business S V3..... 780

 25.5.1.1 Wie Sie permanent lizenzierte Systeme mit CLS Connect auf V3 aktualisieren..... 781

 25.5.1.2 Wie Sie PayGo-lizenzierte Systeme auf V3 aktualisieren..... 782

 25.5.2 Software-Aktualisierung von OpenScape Business S V2 auf OpenScape Business S V3..... 782

25.6 OpenScape Business V2 Netzwerk-Migration/-Aktualisierung auf V3..... 783

 25.6.1 Szenario 1: Hardware-Migration von Master-Knoten, Software-Aktualisierung von Slave-Knoten..... 785

 25.6.1.1 Migration/Aktualisierung mit CLS Connect auf dem Master-Knoten..... 785

 25.6.1.2 Migration/Aktualisierung ohne CLS Connect auf dem Master-Knoten..... 786

 25.6.2 Szenario 2: Software-Aktualisierung aller Systeme im Netzwerk auf V3..... 787

 25.6.2.1 Software-Aktualisierung mit CLS Connect auf dem Master-Knoten..... 787

 25.6.2.2 Software-Aktualisierung ohne CLS Connect auf dem Master-Knoten..... 788

 25.6.3 Szenario 3a: Software-Aktualisierung aller Knoten..... 789

 25.6.4 Szenario 3b: Software-Aktualisierung auf dem Master-Knoten, Hardware-Migration auf den Slave-Knoten..... 789

25.6.4.1 Migration/Aktualisierung mit CLS Connect auf dem Master-Knoten..... 789

25.6.4.2 Migration/Aktualisierung ohne CLS Connect auf dem Master-Knoten..... 790

25.7 Migration von HiPath 3000 auf OpenScape Business V3..... 791

25.7.1 Migration von HiPath 33xx, 35xx, 3800 nach OpenScape Business X3/X5/X8 V3..... 793

25.7.1.1 Wie Sie den KDS aus HiPath 3000 laden..... 798

25.7.1.2 Wie Sie die HG1500 Einstellungen auslesen..... 798

25.7.1.3 Wie Sie den HiPath 3000 KDS konvertieren..... 799

25.7.1.4 Wie Sie die Hardware bei HiPath 3300/3500 austauschen..... 799

25.7.1.5 Wie Sie die Hardware bei HiPath 3350/3550 austauschen..... 801

25.7.1.6 Wie Sie die Hardware bei HiPath 3800 austauschen..... 802

25.7.1.7 Wie Sie die Erstinstallation durchführen..... 803

25.7.1.8 Wie Sie den konvertierten KDS in das neue System laden..... 804

25.7.1.9 Wie Sie eine neue Lizenzdatei generieren..... 805

25.7.1.10 Wie Sie die Lizenzdatei offline aktivieren..... 807

25.7.1.11 Wie Sie Lizenzen zuordnen..... 807

25.7.1.12 Wie Sie die LCR-Einträge zurücksetzen..... 807

25.7.2 Migration eines HiPath 3000 Systems mit OpenScape Office V3 HX auf OpenScape Business V3 mit V3-Mainboard..... 807

25.7.3 Migration eines HiPath 3000 Systems mit OpenScape Office V3 HX auf OpenScape Business V3 mit UC Booster Server..... 809

25.7.3.1 Wie Sie ein OpenScape Office V3 HX Backup-Set konvertieren..... 811

25.7.4 Migration von HiPath 3000 Netzwerk auf OpenScape Business Netzwerk..... 812

25.7.5 Migration eines HiPath 3000 V9 Netzverbands mit HiPath 5000 RSM..... 814

25.7.6 Geänderte/gestrichene Leistungsmerkmale und Schnittstellen von HiPath 3000..... 817

25.8 Migration innerhalb von OpenScape Business V3..... 825

25.9 Migration von HW-Baugruppen..... 826

25.9.1 Ersetzen von SLMO24N durch SLMU..... 826

25.9.2 Ersetzen von SLM8N durch SLMU..... 827

25.9.3 Ersetzen von SLCN durch SLMUC (SLMU + CMAe)..... 827

25.10 Migration von OpenScape Business X1 V2 auf OpenScape Business X1W V3..... 828

25.10.1 Wie Sie permanent lizenzierte Systeme mit CLS Connect auf X1W V3 migrieren..... 829

25.10.2 Wie Sie permanent lizenzierte Systeme ohne CLS Connect auf X1W V3 migrieren.... 830

26 Ausbaugrenzen und Kapazitäten..... 832

26.1 Maximalwerte für Teilnehmer..... 832

26.2 Maximalwerte für Leitungen..... 835

26.3 Maximalwerte der Ressourcen..... 838

26.3.1 Details zur Verwendung von DSP-Kanälen..... 840

26.3.2 Details zur Verwendung von RTP-Proxykanälen..... 841

26.4 Maximalwerte für Leistungsmerkmale..... 842

26.4.1 Anbindung an Service-Provider..... 842

26.4.2 Teilnehmer..... 842

26.4.3 UC Smart-Ausbaustufen..... 842

26.4.4 Smart Voicemail Ausbaustufen..... 846

26.4.5 UC Suite-Ausbaustufen..... 848

26.4.6 Funktionen am Telefon..... 857

26.4.7 Arbeiten im Team (Gruppen)..... 860

26.4.8 Anruf-Routing..... 865

26.4.9 Multimedia Contact Center..... 866

26.4.10 Mobility Ausbaugrenzen..... 867

26.4.11 Sicherheit..... 868

26.4.12 Vernetzung von OpenScape Business..... 869

26.4.13 Anschaltungen..... 870

26.4.14 Application Connectivity..... 870

26.4.15 Gebührenabrechnung..... 873

27 Experten-Modus.....	874
27.1 Darstellungskonventionen für Parameterbeschreibungen.....	874
27.2 Wartung	875
27.2.1 Konfiguration	875
27.2.1.1 Konfiguration > Wartemusik (MoH) > Laden zum Gateway	875
27.2.1.2 Konfiguration > Ansagen > Laden zum Gateway	876
27.2.1.3 Konfiguration > Port-Konfiguration	877
27.2.1.4 Konfiguration > SmartVM	877
27.2.1.5 Konfiguration > SmartVM > Mailbox-Operationen	878
27.2.1.6 Konfiguration > SmartVM > Dateioperationen	878
27.2.1.7 Konfiguration > Branding	881
27.2.1.8 Konfiguration > IP-Gateway-Adresse	881
27.2.2 Software-Image	881
27.2.2.1 Software-Image > System-Software > Update via Internet	881
27.2.2.2 Software-Image > System-Software > Update via File Upload	882
27.2.2.3 Software-Image > System-Software > Update via USB-Stick	883
27.2.2.4 Software-Image > Telefon-Images > Laden	884
27.2.2.5 Software-Image > Telefon-Images > Verteilen	884
27.2.2.6 Software-Image > Telefon-Images > Verteilen pro Endgerät	885
27.2.2.7 Software-Image > Telefon-Logo-Images > Laden	885
27.2.2.8 Software-Image > Telefon-Logo-Images > Verteilen	886
27.2.3 Cordless	886
27.2.3.1 Cordless > Basisstationen	886
27.2.4 Port/Baugruppen Zustand	889
27.2.4.1 Port/Baugruppen Zustand > Baugruppen Zustand	889
27.2.4.2 Port / Baugruppen Zustand > Out of Service	889
27.2.5 Traces	890
27.2.5.1 Traces > Trace-Format-Konfiguration	890
27.2.5.2 Traces > Trace-Ausgabe-Interfaces	892
27.2.5.3 Traces > Trace-Protokoll	892
27.2.5.4 Traces > Digitale Prüfschleife	893
27.2.5.5 Traces > Kunden-Trace-Protokoll	893
27.2.5.6 Traces > M5T-Trace-Komponenten	893
27.2.5.7 Traces > Secure Trace	894
27.2.5.8 Traces > Secure Trace > Secure Trace-Zertifikat	895
27.2.5.9 Traces > Secure Trace > Secure Trace-Einstellungen	895
27.2.5.10 Traces > H.323-Stack-Trace	896
27.2.5.11 Traces > Call Supervision	897
27.2.5.12 Traces > Lizenz-Komponente	899
27.2.5.13 Traces > Trace-Profile	900
27.2.5.14 Traces > Trace-Komponenten	900
27.2.5.15 Traces > TCP Dump	901
27.2.5.16 Traces > rpcap Dämon	902
27.2.5.17 Traces > Kernel-Crash-Daten	902
27.2.5.18 Traces > Medienserver-Trace	903
27.2.6 Events	904
27.2.6.1 Events > Event-Konfiguration	904
27.2.6.2 Ereignisse > Event-Protokoll	904
27.2.6.3 Events > E-Mail	904
27.2.6.4 Events > Reaktionstabelle	905
27.2.6.5 Events > Diagnose Logs	906
27.2.6.6 Events > Alarm-Signalisierung	906
27.2.7 Restart / Reload	907
27.2.7.1 Restart / Reload > Restart / Reload	907
27.2.8 SNMP	909

- 27.2.8.1 **SNMP > Communities** 909
- 27.2.8.2 **SNMP > Communities > Lesende Communities** 909
- 27.2.8.3 **SNMP > Communities > Schreibende Communities** 910
- 27.2.8.4 **SNMP > Communities > Trap Communities** 910
- 27.2.8.5 **SNMP > Traps** 910
- 27.2.9 **Admin-Protokoll**..... 911
 - 27.2.9.1 **Admin-Protokoll > Konfiguration** 911
 - 27.2.9.2 **Admin-Protokoll > Admin-Protokoll-Daten** 911
- 27.2.10 **Aktionen**..... 912
 - 27.2.10.1 **Aktionen > Manuelle Aktionen > Diagnose-Protokolle** 912
 - 27.2.10.2 **Aktionen > Manuelle Aktionen > DLI-Wartung**..... 914
 - 27.2.10.3 **Aktionen > Automatische Aktionen > Garbage Collection** 914
 - 27.2.10.4 **Aktionen > Automatische Aktionen > DLS Notification** 915
 - 27.2.10.5 **Aktionen > Automatische Aktionen > SDHC-Integritätsprüfung**..... 915
- 27.2.11 **Plattform-Diagnose**..... 916
- 27.2.12 **Applikat.-Diagnose**..... 916
 - 27.2.12.1 **Applikat.-Diagnose > Entwickler-Einstellungen > Trace-Konsolen-Ausgabe** 916
 - 27.2.12.2 **Applikat.-Diagnose > Entwickler-Einstellungen > Übernahme des Write Tokens** 916
 - 27.2.12.3 **Applikat.-Diagnose > Mainboard** 916
 - 27.2.12.4 **Applikat.-Diagnose > Entwickler-Einstellungen > SIP-Provider-Profile**..... 916
- 27.2.13 **IP-Diagnose**..... 917
 - 27.2.13.1 **IP-Diagnose > Mainboard > ARP-Protokoll** 917
 - 27.2.13.2 **IP-Diagnose > Mainboard > ICMP-Anforderung > Ping** 917
 - 27.2.13.3 **IP-Diagnose > Mainboard > ICMP-Anforderung > Traceroute** 918
- 27.2.14 **Online-Benutzer**..... 918
 - 27.2.14.1 **Online-Benutzer** 918
- 27.3 **Telefonie**..... 918
 - 27.3.1 **Grundeinstellungen**..... 918
 - 27.3.1.1 **Grundeinstellungen > System > System Flags**..... 919
 - 27.3.1.2 **Grundeinstellungen > System > Zeitarameter** 928
 - 27.3.1.3 **Grundeinstellungen > System > Display**..... 934
 - 27.3.1.4 **Grundeinstellungen > System > DISA** 938
 - 27.3.1.5 **Grundeinstellungen > System > Abwurf/Attendant/Hotline** 939
 - 27.3.1.6 **Grundeinstellungen > System > LDAP**..... 942
 - 27.3.1.7 **Grundeinstellungen > System > Texts** 943
 - 27.3.1.8 **Grundeinstellungen > System > Flexible Menüs** 944
 - 27.3.1.9 **Grundeinstellungen > System > Kurzwahlziele** 944
 - 27.3.1.10 **Grundeinstellungen > System > Service Codes** 946
 - 27.3.1.11 **Grundeinstellungen > System > HFA-Registrierungs-Passwort**..... 946
 - 27.3.1.12 **Grundeinstellungen > Gateway** 947
 - 27.3.1.13 **Grundeinstellungen > DynDNS > DynDNS Service** 948
 - 27.3.1.14 **Grundeinstellungen > DynDNS > Aktualisierungszeit der DNS-Namen** .. 949
 - 27.3.1.15 **Grundeinstellungen > Quality of Service** 950
 - 27.3.1.16 **Grundeinstellungen > Datum und Uhrzeit > Datum und Uhrzeit** 951
 - 27.3.1.17 **Grundeinstellungen > Datum und Uhrzeit > Zeitzonen-Einstellungen** ... 951
 - 27.3.1.18 **Grundeinstellungen > Datum und Uhrzeit > SNTP-Einstellungen** 952
 - 27.3.1.19 **Grundeinstellungen > Port-Verwaltung** 952
 - 27.3.1.20 **Grundeinstellungen > Gebühren > Gebühren Ausgabe** 953
 - 27.3.1.21 **Grundeinstellungen > Gebühren > Gebühren Faktoren** 955
 - 27.3.1.22 **Grundeinstellungen > Gebühren > Gebühren Projekt Kennzahlen** 957
 - 27.3.1.23 **Grundeinstellungen > Wiedergabegerät für Sprachnachrichten/ Ansagen** 957
 - 27.3.1.24 **Grundeinstellungen > Telefonparameter-Bereitstellung**..... 957
 - 27.3.1.25 **Grundeinstellungen > Power Management** 960

- 27.3.1.26 Grundinstallation > Massendaten..... 961
- 27.3.2 **Sicherheit**..... 962
 - 27.3.2.1 **Sicherheit > Application Firewall** 962
 - 27.3.2.2 **Sicherheit > Deployment- und Licensing-Client (DLSC)** 963
 - 27.3.2.3 **Sicherheit > Deployment- und Licensing-Client (DLSC) > DLSC Client-Zertifikat** 964
 - 27.3.2.4 **Sicherheit > Deployment- und Licensing-Client (DLSC) > DLSC CA - Zertifikat** 965
 - 27.3.2.5 **Sicherheit > Signaling- und Payload-Encryption** 967
 - 27.3.2.6 **Sicherheit > Signaling- und Payload-Encryption > SPE-Zertifikat** 968
 - 27.3.2.7 **Sicherheit > Signaling- und Payload-Encryption > SPE CA-Zertifikate** 968
 - 27.3.2.8 **Sicherheit > VPN** 969
 - 27.3.2.9 **Sicherheit > VPN > Lightweight CA** 969
 - 27.3.2.10 **Sicherheit > VPN > Zertifikatsverwaltung** 970
 - 27.3.2.11 **Sicherheit > VPN > Zertifikatsverwaltung > Trusted CA Zertifikate > Aktive Zertifikate** 971
 - 27.3.2.12 **Sicherheit > VPN > Zertifikatsverwaltung > Trusted CA Zertifikate > Konfigurierte Zertifikate** 972
 - 27.3.2.13 **Sicherheit > VPN > Peer-Zertifikate** 972
 - 27.3.2.14 **Sicherheit > VPN > Dienste > Aktive Dienste** 974
 - 27.3.2.15 **Sicherheit > VPN > Dienste > Konfigurierte Dienste** 974
 - 27.3.2.16 **Sicherheit > VPN > Tunnel > Aktive Tunnel** 975
 - 27.3.2.17 **Sicherheit > VPN > Tunnel > Konfigurierte Tunnel** 978
 - 27.3.2.18 **Sicherheit > VPN > Regeln > Aktive Regeln** 983
 - 27.3.2.19 **Sicherheit > VPN > Regeln > Konfigurierte Regeln** 984
 - 27.3.2.20 **Sicherheit > VPN > Public Key Infrastructure (PKI)** 986
 - 27.3.2.21 **Sicherheit > SSL > Zertifikatsgenerierung** 986
 - 27.3.2.22 **Sicherheit > SSL > Zertifikatsverwaltung** 987
 - 27.3.2.23 **Sicherheit > SSL > Zertifikatsverwaltung > Server-Zertifikate** 988
 - 27.3.2.24 **Sicherheit > Web Sicherheit** 989
 - 27.3.2.25 **Sicherheit > SQL Sicherheit** 989
- 27.3.3 **Netzwerkschnittstellen**..... 990
 - 27.3.3.1 **Netzwerkschnittstellen > Mainboard > Host-Name** 990
 - 27.3.3.2 **Netzwerkschnittstellen > Mainboard > LAN 1 (WAN)**..... 990
 - 27.3.3.3 **Netzwerkschnittstellen > Mainboard > LAN 2**..... 995
 - 27.3.3.4 **Netzwerkschnittstellen > Mainboard > LAN 3 (Admin)**..... 996
 - 27.3.3.5 **Netzwerkschnittstellen > Mainboard > FTP-Server** 997
 - 27.3.3.6 **Netzwerkschnittstellen > Mainboard > DHCP Modus** 998
 - 27.3.3.7 **Netzwerkschnittstellen > Mainboard > DHCP Modus > DHCP-Server > Globale Parameter** 998
 - 27.3.3.8 **Netzwerkschnittstellen > Mainboard > DHCP-Modus > DHCP-Server > IP-Adressen-Pools** 1000
 - 27.3.3.9 **Netzwerkschnittstellen > Mainboard > DHCP-Modus > DHCP-Server > Statische IP-Adressen** 1001
 - 27.3.3.10 **Netzwerkschnittstellen > Mainboard > DHCP-Modus > DHCP-Server > Zuletzt aktive Leases** 1002
 - 27.3.3.11 **Netzwerkschnittstellen > Mainboard > DHCP Modus > DHCP Server > Alle Leases** 1003
 - 27.3.3.12 **Netzwerkschnittstellen > Application Board > Host-Name** 1003
 - 27.3.3.13 **Netzwerkschnittstellen > Application Board > LAN 1**..... 1004
 - 27.3.3.14 **Netzwerkschnittstellen > Application Board > LAN 2**..... 1005
- 27.3.4 **Routing**..... 1006
 - 27.3.4.1 **Routing > IP-Routing > Mainboard > Statische Routen** 1006
 - 27.3.4.2 **Routing > IP-Routing > Mainboard > Default Router** 1006
 - 27.3.4.3 **Routing > IP-Routing > Mainboard > DNS-Server** 1007
 - 27.3.4.4 **Routing > IP-Routing > Application Board > Statische Routen** 1007

- 27.3.4.5 **Routing > IP-Routing > Application Board > Default Router**1008
- 27.3.4.6 **Routing > NAT** 1008
- 27.3.4.7 **Routing > PSTN** 1009
- 27.3.4.8 **Routing > PSTN > PPP-Protokoll**1010
- 27.3.4.9 **Routing > PSTN > PSTN-Partner** 1010
- 27.3.5 **LCR**.....1014
 - 27.3.5.1 **LCR > LCR-Flags**1014
 - 27.3.5.2 **LCR > Berechtigungen** 1015
 - 27.3.5.3 **LCR > Wahlplan** 1015
 - 27.3.5.4 **LCR > Wegetabelle**1016
 - 27.3.5.5 **LCR > Wahlregel** 1018
 - 27.3.5.6 **LCR > Multisite** 1020
- 27.3.6 **Sprachgateway**.....1021
 - 27.3.6.1 **Sprachgateway > SIP-Parameter** 1021
 - 27.3.6.2 Sprachgateway > ITSP Loc-ID Einstellungen.....1023
 - 27.3.6.3 **Sprachgateway > Codec-Parameter** 1024
 - 27.3.6.4 **Sprachgateway > Ziel-Codec-Parameter**1027
 - 27.3.6.5 **Sprachgateway > Internet-Telefonie Service Provider**..... 1027
 - 27.3.6.6 **Sprachgateway > Networking > Knoten**1039
 - 27.3.6.7 **Sprachgateway > Networking > Routing**1039
 - 27.3.6.8 **Sprachgateway > SIPQ-Verbindung** 1040
 - 27.3.6.9 **Sprachgateway > Native SIP Server-Trunk**.....1041
- 27.3.7 **Teilnehmer**.....1047
 - 27.3.7.1 **Teilnehmer > Teilnehmer > UPO Teilnehmer**.....1047
 - 27.3.7.2 **Teilnehmer > Teilnehmer > IP Clients**1050
 - 27.3.7.3 **Station > Station > Analog Stations**1052
 - 27.3.7.4 **Teilnehmer > Teilnehmer > ISDN-Teilnehmer** 1054
 - 27.3.7.5 **Teilnehmer > Teilnehmer > DECT-Teilnehmer > SLC-Rufnummer** 1055
 - 27.3.7.6 **Teilnehmer > Teilnehmer > DECT-Teilnehmer > DECT-Teilnehmer**1056
 - 27.3.7.7 **Teilnehmer > Teilnehmer > IVM/EVM Ports > EVM** 1058
 - 27.3.7.8 **Teilnehmer > Teilnehmer > Virtuale Teilnehmer** 1059
 - 27.3.7.9 **Teilnehmer > Teilnehmer > Teilnehmer-Parameter**.....1060
 - 27.3.7.10 **Teilnehmer > Teilnehmer > UC-Anwendungen** 1072
 - 27.3.7.11 **Teilnehmer > Teilnehmer > Profile/Vorlagen** 1073
 - 27.3.7.12 **Teilnehmer > Teilnehmer > Durchwahl Rufnummern**1075
 - 27.3.7.13 **Teilnehmer > Teilnehmer > Mobility Entry** 1075
 - 27.3.7.14 **Teilnehmer > Teilnehmer > Circuit-Teilnehmer**.....1077
 - 27.3.7.15 **Station > Station > Sfb-Benutzer**.....1078
 - 27.3.7.16 **Teilnehmer > Teilnehmer > Übersicht Teilnehmer** 1079
 - 27.3.7.17 **Teilnehmer > Tastenprogrammierung** 1080
- 27.3.8 **Cordless**.....1081
 - 27.3.8.1 **Cordless > Systemweit**1081
 - 27.3.8.2 **Cordless > SLC**1083
 - 27.3.8.3 **Cordless > Multi-SLC** 1084
 - 27.3.8.4 **Cordless > Basisstationen** 1085
- 27.3.9 **Kommende Rufe**.....1085
 - 27.3.9.1 **Kommende Rufe > Gruppen-/Sammelanschluss**1086
 - 27.3.9.2 **Kommende Rufe > Gruppen-Teilnehmer**1089
 - 27.3.9.3 **Kommende Rufe > Team/Top** 1091
 - 27.3.9.4 **Kommende Rufe > Anrufübernahme** 1094
 - 27.3.9.5 **Kommende Rufe > UCD** 1095
 - 27.3.9.6 **Kommende Rufe > Rufweitzerschaltungen**.....1098
- 27.3.10 **Leitungen/Vernetzung**.....1100
 - 27.3.10.1 **Leitungen/Vernetzung > Leitungen** 1100
 - 27.3.10.2 **Trunks/Routing > Trunk group**..... 1104
 - 27.3.10.3 **Leitungen/Vernetzung > QSIG-Leistungsmerkmale** 1112

- 27.3.10.4 Leitungen/Routing > MSN zuweisen 1114
- 27.3.10.5 Leitungen/Vernetzung > ISDN-Parameter1114
- 27.3.11 Berechtigungen (Classes of Service)..... 1114
 - 27.3.11.1 Berechtigungen > Teilnehmer 1115
 - 27.3.11.2 Berechtigungen > Tag: Berechtigungsgruppen 1115
 - 27.3.11.3 Berechtigungen > Nacht: Berechtigungsgruppen 1116
 - 27.3.11.4 Berechtigung > Erlaubnislisten1117
 - 27.3.11.5 Berechtigungen > Verbotslisten 1117
 - 27.3.11.6 Berechtigungen > Blacklist1118
 - 27.3.11.7 Berechtigungen > Nachtschaltung 1119
 - 27.3.11.8 Berechtigungen > VBZ Gruppenzuordnung 1119
 - 27.3.11.9 Berechtigungen > CON Matrix 1120
 - 27.3.11.10 Berechtigungen > Automatische Nachtschaltung..... 1121
 - 27.3.11.11 Berechtigungen > Sondertage..... 1121
- 27.3.12 Anschaltungen..... 1122
 - 27.3.12.1 Anschaltungen > Ansage/Interne Wartemusik > Ansagen und
Wartemusik 1122
 - 27.3.12.2 Anschaltungen > Türsprechstelle (Türöffner) 1123
 - 27.3.12.3 Anschaltungen > SmartVM 1124
- 27.3.13 Payload.....1128
 - 27.3.13.1 Payload > Devices 1128
 - 27.3.13.2 Payload > Media Stream Control (MSC) 1128
 - 27.3.13.3 Payload > HW-Module 1129
- 27.3.14 Statistiken..... 1132
 - 27.3.14.1 Statistik > Gateway-Statistik > Mainboard > Device-Statistik 1132
 - 27.3.14.2 Statistiken > Gateway-Statistiken > Mainboard > MSC-Statistiken 1133
 - 27.3.14.3 Statistiken > SNMP-Statistiken 1134
 - 27.3.14.4 Statistiken > Telephonie Statistiken > System Texte 1134
 - 27.3.14.5 Statistiken > Telephonie Statistiken > UCD Agenten 1134
 - 27.3.14.6 Statistiken > Telephonie Statistiken > TZustand Leitung..... 1135
 - 27.3.14.7 Statistiken > Telephonie Statistiken > Weiterleitung 1135
 - 27.3.14.8 Statistiken > Telephonie Statistiken > Teilnehmer 1136
- 27.4 Applikationen..... 1137
 - 27.4.1 Applikationsauswahl..... 1137
 - 27.4.1.1 Applikationsauswahl 1137
 - 27.4.2 Active Directory Integration Service..... 1138
 - 27.4.2.1 Active Directory Integration Service..... 1138
 - 27.4.3 UC Smart.....1139
 - 27.4.3.1 UC Smart > Grundeinstellungen 1139
 - 27.4.3.2 UC Smart > Benutzerverwaltung..... 1140
 - 27.4.3.3 UC Smart > -Status..... 1141
 - 27.4.4 OpenScape Business, UC Suite..... 1141
 - 27.4.4.1 OpenScape Business, UC Suite 1141
 - 27.4.4.2 OpenScape Business, UC Suite > Benutzerverzeichnis..... 1142
 - 27.4.4.3 OpenScape Business, UC Suite > Abteilungen..... 1145
 - 27.4.4.4 OpenScape Business, UC Suite > Gruppen..... 1145
 - 27.4.4.5 OpenScape Business UC Suite > Templates..... 1147
 - 27.4.4.6 OpenScape Business UC Suite > Externes Verzeichnis..... 1147
 - 27.4.4.7 OpenScape Business UC Suite > Externer Anbieter..... 1148
 - 27.4.4.8 OpenScape Business UC Suite > Contact Center..... 1150
 - 27.4.4.9 OpenScape Business UC Suite > Zeitpläne..... 1159
 - 27.4.4.10 OpenScape Business UC Suite > Datei-Upload..... 1161
 - 27.4.4.11 OpenScape Business UC Suite > Konferenzschaltung..... 1162
 - 27.4.4.12 OpenScape Business UC Suite > Standort-Liste 1162
 - 27.4.4.13 OpenScape Business UC Suite > Server..... 1163
 - 27.4.4.14 OpenScape Business, UC Suite > Profile..... 1170

27.4.4.15	OpenScape Business, UC Suite > Faxkopfzeilen	1172
27.4.4.16	OpenScape Business UC Suite > Skin-Einstellungen	1172
27.4.5	Web Services	1173
27.4.5.1	Web Services > Web Collaboration	1173
27.4.6	Open Directory Service	1174
27.4.6.1	Open Directory Service > Grundeinstellungen	1174
27.4.6.2	Open Directory Service > Datenquellen > OpenScape Business	1174
27.4.6.3	Open Directory Service > Datenquellen > LXV3	1174
27.4.6.4	Open Directory Service > Datenquellen > LXV3	1175
27.4.6.5	Open Directory Service > Wartung	1175
27.4.6.6	OpenStage Gate View	1175
27.4.7	OpenStage Gate View	1175
27.4.8	Application Launcher	1176
27.4.8.1	Application Launcher	1176
27.5	Middleware	1176
27.5.1	Wiedergabegerät für Ansagen	1176
27.5.2	Csta Message Dispatcher (CMD)	1176
27.5.3	Csta Service Provider (CSP)	1177
27.5.4	DSS-Server	1178
27.5.5	Media Extension Bridge (MEB)	1178
28	Anhang	1179
28.1	Unterstützte Standards.....	1179
28.2	Euro-ISDN-Leistungsmerkmale.....	1181
28.3	Verwendete Ports.....	1183
28.4	Projektierung der DSP-Kanäle für die Kommunikationssysteme OpenScape Business X3/X5/ X8.....	1185
29	Glossar	1197
29.1	Glossar.....	1197
Index		1214

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.

Tipp: 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 Hardwaremodelle OpenScape Business X1, OpenScape Business X3, OpenScape Business X5 und OpenScape Business X8 sowie das Softwaremodell OpenScape Business S (Softswitch). Die UC-Lösung UC Smart ist auf allen OpenScape Business Modellen integriert. Die UC-Lösung UC Suite wird für die Hardwaremodelle mit der optionalen UC Booster Card oder dem UC Booster Server geboten; beim Softswitch kann zwischen UC Smart oder UC Suite gewählt werden.

Anmerkung: Die Hardwaremodelle 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 Projektplanung

Die folgenden Dokumentationen richten sich an Vertrieb und Projektplanung.

- Leistungsmerkmalbeschreibung
Diese Dokumentation beschreibt sämtliche Leistungsmerkmale. Dieses Dokument ist ein Auszug aus der Administratordokumentation.

Installation und Service

Die folgenden Dokumentationen richten sich an Servicetechniker.

- OpenScape Business X1/X1W, Installationsanleitung
Diese Dokumentation beschreibt die Montage der Hardware und die Erstinstallation von OpenScape Business X1.
- OpenScape Business X3/X5/X8, Installationsanleitung
Diese Dokumentation beschreibt die Montage der Hardware und die Erstinstallation von OpenScape Business X3/X5/X8.
- OpenScape Business S, Installationsanleitung
Diese Dokumentation beschreibt die Erstinstallation des Softswitchs OpenScape Business S.
- OpenScape Business X1/X1W, Servicedokumentation
Diese Dokumentation beschreibt die Hardware von OpenScape Business X1.
- OpenScape Business X3/X5/X8, Servicedokumentation
Diese Dokumentation beschreibt die Hardware von OpenScape Business X3/X5/X8.

Administration

Die folgenden Dokumentationen richten sich an Administratoren.

- Administratordokumentation
Diese Dokumentation beschreibt die Konfiguration der Leistungsmerkmale, die über den OpenScape Business Assistant (WBM) eingerichtet werden. Die Administratordokumentation ist im System als Online-Hilfe verfügbar.
- Konfiguration für Kundenadministratoren, Administratordokumentation
Diese Dokumentation beschreibt die Konfiguration der Leistungsmerkmale, die über den OpenScape Business Assistant (WBM) mit dem Administratorprofil **Basic** eingerichtet werden können.
- Manager E, Administratordokumentation
Diese Dokumentation beschreibt die Konfiguration der Leistungsmerkmale, die über den Manager E eingerichtet werden.

UC Clients / Telefon User Interfaces (TUI)

Die folgenden Dokumentationen richten sich an UC Benutzer.

- myPortal for Desktop, Bedienungsanleitung
Diese Dokumentation beschreibt die Installation, Konfiguration und Bedienung des UC Clients myPortal for Desktop.
- myPortal for Outlook, Bedienungsanleitung
Diese Dokumentation beschreibt die Installation, Konfiguration und Bedienung des UC Clients myPortal for Outlook.
- myPortal@work, Benutzerhandbuch
Diese Dokumentation beschreibt die Installation, Konfiguration und Bedienung des UC Clients myPortal @work.
- Fax Printer, Bedienungsanleitung
Diese Dokumentation beschreibt die Installation, Konfiguration und Bedienung von Fax Printer.
- myPortal to go, Bedienungsanleitung
Diese Dokumentation beschreibt die Konfiguration und Bedienung des mobilen UC Clients myPortal to go für Smartphones und Tablet-PC.
- myAgent, Bedienungsanleitung
Diese Dokumentation beschreibt die Installation, Konfiguration und Bedienung des Contact Center Clients myAgent.
- myReports, Bedienungsanleitung
Diese Dokumentation beschreibt die Installation, Konfiguration und Bedienung des Contact Center Clients myReports.
- myAttendant, Bedienungsanleitung
Diese Dokumentation beschreibt die Installation, Konfiguration und Bedienung des Vermittlungsplatzes myAttendant.
- OpenScape Business Attendant, Bedienungsanleitung
Diese Dokumentation beschreibt die Installation, Konfiguration und Bedienung des Vermittlungsplatzes OpenScape Business Attendant.
- UC Smart Telefon User Interface (TUI), Kurzbedienungsanleitung
Diese Dokumentation beschreibt das Sprachbox-Telefonmenü der UC-Lösung UC Smart.
- UC Suite Telefon User Interface (TUI), Kurzbedienungsanleitung
Diese Dokumentation beschreibt das Sprachbox-Telefonmenü der UC-Lösung UC Suite.

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

Einführung und wichtige Hinweise

Kapitel	Inhalt
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
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 to go, Mobility Entry, One Number Service, Dual-Mode-Telefonie, IP-Mobility, Cordless/DECT
Sicherheit	Firewall, SPE, VPN, Zertifikate
Vernetzung von OpenScape Business	Vernetzungsplan, Vernetzungsszenarien, Zentraler Abwurfplatz, Survivability
Anschaltungen	Ansagegeräte, Türsprechstelle und Türöffner, Aktoren und Sensoren
Application Connectivity	CSTA, TAPI, Application Launcher
Gebührenabrechnung	Gesprächsdatenerfassung, Gebühren und Gesprächsdauer, Kostenkontrolle
Wartung	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 Kommunikationssysteme
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

1.1.3 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 ...

1.1.4 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 <i>Netzwerk</i> .
Ausgabe	Schriftart mit fester Laufweite, z. B. Courier	Befehl nicht gefunden.
Eingabe	Schriftart mit fester Laufweite, z. B. Courier	LOCAL als Dateiname eingeben
Tastaturkombination	Schriftart mit fester Laufweite, z. B. Courier	<Strg>+<Alt>+<Esc>

Einführung und wichtige Hinweise

Sicherheits- und Warnhinweise

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.



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



VORSICHT: Kennzeichnet gefährliche Situation, die Verletzungen zur Folge haben kann.

Anmerkung: 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

Zugehörige Konzepte

[Wichtige Hinweise](#) auf Seite 39

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.



Achtung: 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 Kommunikationssystem 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.

Einführung und wichtige Hinweise

- 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 Warnungen: Vorsicht

Warnhinweise des Typs Vorsicht kennzeichnen eine gefährliche Situation, die Verletzungen zur Folge haben 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: 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.

Einführung und wichtige Hinweise

- 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 Notfalleinrufe 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 Notfalleinrufe 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 Software and Solutions 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 frühesten 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

Einführung und wichtige Hinweise

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 Software and Solutions 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 Software and Solutions 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, Krankenzimmern, 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 Software and Solutions GmbH & Co. KG sind kompatibel mit Hörhilfen und erfüllen die Anforderungen gemäß den FCC-Vorschriften, Teil 68, Abschnitt 68.316/68.317.

- Programmierte Wählfunktionen

Wenn Sie Notrufnummern programmieren oder über ein Produkt der Unify Software and Solutions 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 Software and Solutions GmbH & Co. KG ohne ordnungsgemäße Rufannahme-Überwachung betreiben, verstoßen gegen Teil 68 der FCC-Vorschriften.

Die in dieser Dokumentation beschriebenen Kommunikationssysteme der Unify Software and Solutions 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 Software and Solutions 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 Zugangscodes 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 Software and Solutions 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

Die Kennzeichnung durch „Innovation, Science and Economic Development Canada (ISED)“ weist zertifizierte Geräte aus. 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. „Innovation, Science and Economic Development Canada (ISED)“ 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 Funkstöreeigenschaften der Kommunikationssysteme und über Datenschutz und Datensicherheit.

Zugehörige Konzepte

[Sicherheits- und Warnhinweise](#) auf Seite 30

1.3.1 Verhalten in Notfällen

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

Vorgehensweise bei Unfällen

Erste Hilfe Maßnahmen

Notruf

Meldung von 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.
- 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.

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

- Wo geschah was?

Einführung und wichtige Hinweise

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

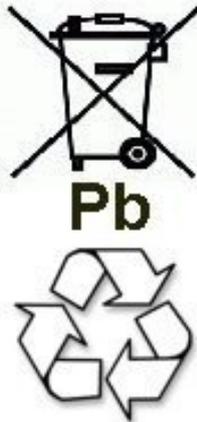
Anmerkung: Reinigen Sie das Gehäuse von Kommunikationssystem und Server nur mit einem weichen, leicht feuchten Tuch. Benutzen Sie keine scharfen Reiniger oder Scheuerschwämme.

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 2012/19/EU 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 Office 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

Einführung und wichtige Hinweise

Schutz- und Neutralleiter aufgeteilt ist. TN-S und TN-C-S gemäß Definition der Norm IEC 60364-1 und IEC60364-5-51

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.^{***)}

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 Prüfmethode UL VW-1	EN 60332-1-1 und EN 60332-2-1	DIN EN 60332-1-1 (VDE 0482-332-1-1) und DIN EN 60332-2-1 (VDE 0482-332-2-1)
--	-------------------------------	---

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 *OpenScape Business Installationsanleitung*.

*) 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).

Anmerkung: 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.

Anmerkung:

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 55032.

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.

Tipp: 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 Software and Solutions 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 Sicherheits-CDs-/DVDs oder Protokollausdrucke. Das gilt sowohl für den Serviceeinsatz, als auch für Lagerung und Transport.

Einführung und wichtige Hinweise

- 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

Die CE-Zertifizierung beruht auf: 2014/35/EU - Niederspannungsrichtlinie (LVD); (Amtsblatt der EU L96 vom 29.03.2014, S. 357-374) 2014/30/EU - Richtlinie über die elektromagnetische Verträglichkeit (EMV); (Amtsblatt der EU L96 vom 29.03.2014, S. 79-106) 2011/65/EU - Richtlinie zur Beschränkung der Verwendung bestimmter gefährlicher Stoffe (RoHS); (Amtsblatt der EU L174 vom 01.07.2011, S. 88-110)

	Normenreferenz
Safety	EN 62368-1
Electromagnetic Compatibility EMC	EN55032 (EMC Emission) EN55024 (EMC Immunity Residential)

1.3.7.2 Konformität mit US- und kanadischen Normen

	Normenreferenz
Safety USA and Canada	CSA/UL 62368-1
EMC Emission Canada	ICES-003 Issue 6 Class B
EMC Emission USA	FCC 47 CFR Part 15 Subpart B 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 und IEC 62368-1
EMC Emission	CISPR 32

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 H₂O/m³
- 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.

Anmerkung: Schäden durch lokale Temperaturerhöhungen

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

Anmerkung: 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

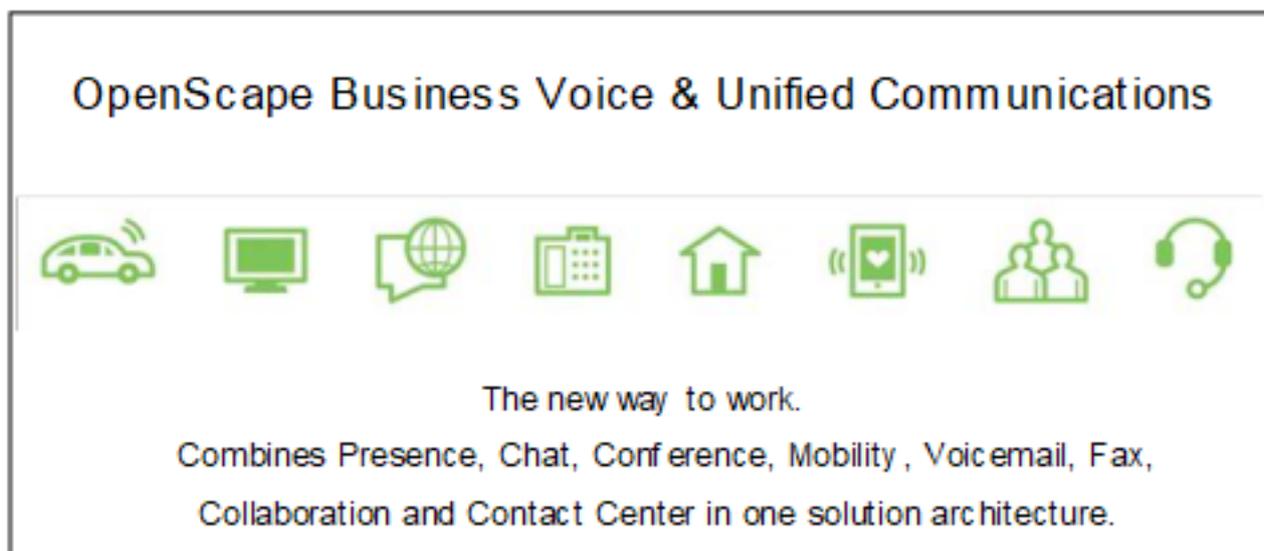
Angaben zu den klimatischen und mechanischen Bedingungen für den Betrieb von OpenScape Business S und OpenScape Business UC Booster Server (Application Server) entnehmen Sie bitte den Herstellerunterlagen der Server-PCs und der weiteren Komponenten.

2 Systemübersicht

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 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. Alternativ besteht die Möglichkeit die OpenScape Business Software auf einem Standard-Server zu betreiben (Softswitch) - selbstverständlich auch in voll virtualisierten Umgebungen.
- Die UC-Lösung UC Smart ist bereits auf dem Mainboard vorgeleistet. Die additive UC-Lösung UC Suite unterstützt eine größere Anzahl von UC Benutzern und bietet einen erweiterten UC-Leistungsumfang. Dafür ist eine UC Booster Card oder ein UC Booster Server notwendig.
- für die vielseitigen und heterogenen Anforderungen sind alle Kommunikationsschnittstellen bereits vorhanden: IP, digital, analog und DECT sowie alle gängigen Amtsschnittstellen 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 in OpenScape Business integrierte UC-Smart-Lösung kann jederzeit über eine Upgrade-Lizenz auf die erweiterte UC-Suite-Lösung migriert werden. Je nach Anzahl der UC-Teilnehmer muss dann OpenScape Business nur noch durch die interne Baugruppe "UC Booster Card" oder mit den externen Linux-Server "UC Booster Server" erweitert werden. Als reiner Softswitch steht die OpenScape Business S als Server-Lösung mit wahlweise UC Smart oder 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 für Sie geeignete UC-Lösung auszuwählen. Detaillierte funktionale Einschränkungen finden Sie in den entsprechenden Kapiteln (UC Smart, UC

Suite, Attendants) der Leistungsmerkmalbeschreibung bzw. Administratordokumentation.

UC-Funktion	UC Smart	UC Suite			Bemerkungen
	myPortal to go	myPortal for Desktop/ Outlook	myPortal @work	myPortal to go	
Anwesenheitsstatus					
Anwesenheitsstatus (Präsenz-Management)	x	x	x	x	
Änderung des Anwesenheitsstatus über Client	x	x	x	x	
Änderung des Anwesenheitsstatus über TUI	-	x	-	-	
Statusbezogene Anrufumleitung	x	x	x	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	
Statusanzeige in Verzeichnissen	x	x	x	x	
Statusanzeige im Journal	-	x	-	-	
CallMe aktivieren	-	x	x	x	
Kalender-Integration (Outlook)	-	x	-	-	
Kalenderintegration (iCal) (nur mit myPortal for Desktop)	-	x	-	-	
Favoriten					
Anzeige des Anrufstatus	x	x	x	x	
Anlegen von Gruppen	x	x	-	-	
Kompakte Anzeige der Favoriten	-	x	-	-	

Systemübersicht

UC-Funktion	UC Smart	UC Suite			Bemerkungen
	myPortal to go	myPortal for Desktop/ Outlook	myPortal @work	myPortal to go	
Verzeichnisse					
Persönliches Verzeichnis	x	x	x	x	
Internes Verzeichnis	x	x	x	x	
Externes Verzeichnis	-	x	x	x	
Suche in den Verzeichnissen	x	x	x	x	
Zugriff auf im System definierte Kurzwahlziele (KWZ)	x	-	x	x	
Import / Verwalten persönlicher Kontakte (CSV/ XML)	-	x	-	-	
Zugriff auf Outlook-Kontakte	-	x	-	-	
Import von persönlichen Kontakten (Mac OS) (myPortal for Desktop)	-	x	-	-	
Integration externer Verzeichnisse über LDAP	-	x	-	-	
Journal					
Alle Anrufe	x	x	-	x	
Offene Anrufe	-	x	-	-	
Entgangene Anrufe	x	x	-	x	
Angenommene Anrufe	x	x	-	x	
Geplante Anrufe	-	x	-	-	
Voicemail	x	x	-	x	
Fax-Journal	-	x	-	-	
Gespräche					
Chat	-	-	-	-	
Journal	-	-	x	-	
Voicemail	-	-	x	-	
Anrufe					
Manuelle Wahl	x	x	x	x	
Desktop-Wahl (Click to Call)	-	x	-	-	
Umleiten	x	x	x	x	
Anruf halten	x	x	x	x	

UC-Funktion	UC Smart	UC Suite		Bemerkungen	
	myPortal to go	myPortal for Desktop/ Outlook	myPortal @work		myPortal to go
Aufzeichnen von Anrufen (Voice Recording)	-	X	-	-	
E-Mail senden	X	X	X	X	
SMS senden	X	-	-	X	
Chat starten	-	X	-	-	
Popups	-	X	-	-	
Konferenzen					
AdHoc-Konferenz	X	X	X	X	
Geplante Konferenzen	-	X	-	-	
Permanente und offene Konferenzen (Drag&Drop-Konferenz)	-	X	-	-	
Web Collaboration-Einbindung	-	X			
Sprach- und Faxnachrichten					
Sprachbox (Visuelle Voicemail)	X	X	X	X	VoiceMail-Funktionalität für Teilnehmer (IP, TDM)
Abhören über Telefon	X	X	X	X	
Abhören über PC-Soundkarte	-	X	-	-	
Wie Sie eine Sprachnachricht als E-Mail senden	X	X	-	-	
Fax	-	X	-	-	
Instant Messaging					
Instant Messaging (Chat)	-	X	-	-	

1 myPortal to go ermöglicht auch den Zugriff auf die lokalen Smartphone-Kontakte.

Contact Center

UC-Funktion	UC Smart	UC Suite		Bemerkungen
		myAgent	myReports	
Agenten, Warteschlangen und Zeitpläne	-	X	-	
Fax und E-Mail	-	X	-	

Systemübersicht

UC-Funktion	UC Smart	UC Suite		Bemerkungen
		myAgent	myReports	
vordefinierte Reports/ Berichtsvorlagen	-	x	x	
Zeitgesteuertes Erstellen von Reports/Berichten	-	-	x	

Optional ist die Anschaltung von OpenScape Contact Center möglich.

Attendants (Vermittlungsplätze)

UC-Funktion	UC Smart	UC Suite	Bemerkungen
	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 anderer 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-Zugang	x	x	
Journal	-	x	
AdHoc-Konferenz	x	x	
Geplante, permanente und offene Konferenzen (Drag&Drop-Konferenz)	-	x	

UC-Funktion	UC Smart	UC Suite	Bemerkungen
	Business Attendant	myAttendant	
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	

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

VoiceMail & Company AutoAttendant

UC-Funktion	UC Smart	UC Suite	Bemerkung
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	

Systemübersicht

UC-Funktion	UC Smart	UC Suite	Bemerkung
Company AutoAttendant	x	x	Zentraler Vermittlungsplatz und zentrale Voicemail mit alternativen Ansagen je Nebenstelle
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. AutoAttendant	-	x	Präsenzabhängige Rufbehandlung individuell je Teilnehmer einstellbar
Zeitpläne	Tag-Nachschaltung	Zeitplan mit Regeln (Call Control Vector CCV)	
Vorlagen (Templates)	1 AutoAttendant standardmäßig eingerichtet	5 anpassbare Vorlagen	
grafischer Regel-Editor (CCV-Editor)	-	x	
Verkettung von Mailboxen / Multi Step AutoAttendant	x	-	Das Gespräch wird von einer verketteten Mailbox auf die nächste weitergeleitet und dabei wird immer die jeweilige Ansage abgespielt
Nach Name wählen	-	x	
Nebenstellenwahl	x	x	
Voicemail-Funktionen			

UC-Funktion	UC Smart	UC Suite	Bemerkung
Individuelle Begrüßungen pro Mailbox	4	10	Verschiedene Ansagen speichern und einstellen
Weiterleiten 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
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 In OpenScape Business S, in dem eine Live-Aufzeichnung von UC verwendet wird, wird G.729A nicht berücksichtigt.
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

Zugehörige Konzepte

[UC Smart](#) auf Seite 230

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 @work	x	x	UC-Desktop-Client für Microsoft Windows und Mac OS X
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
OpenScape Desk Phone CP 400/600/600E/700/700X/710 HFA (in der Telefon-Software integrierter Client)	x	x	Präsenz-Steuerung und Zugriff auf das Telefonbuch bei UC Suite und UC Smart

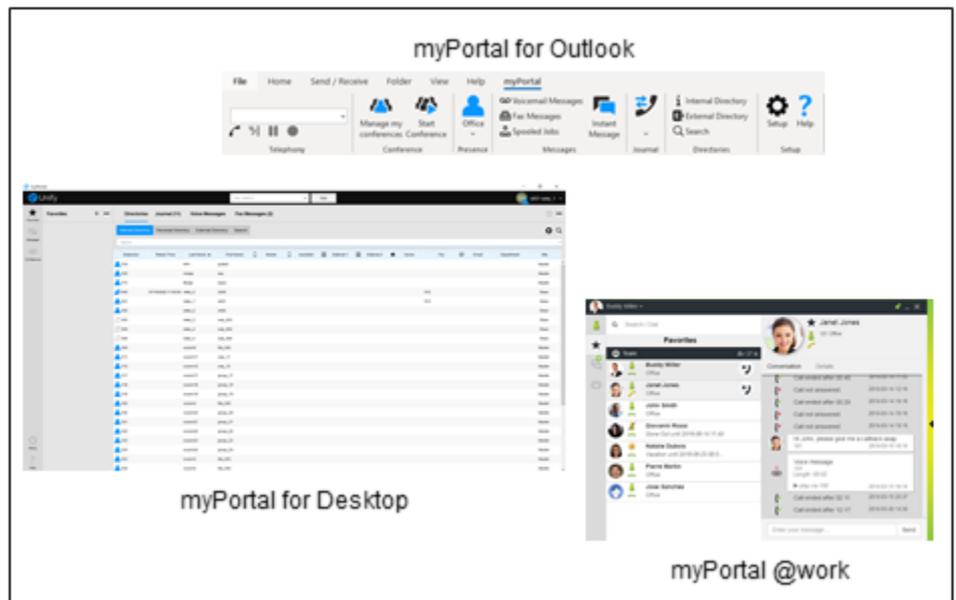


Abbildung 1: myPortal for Desktop, myPortal for Outlook und myPortal @work

Mobility Clients

Client	Empfohlen für		Beschreibung
	UC Smart	UC Suite	
myPortal to go	x	x	Mobile App für Smartphones und Tablet-PC myPortal to go ist mit leicht unterschiedlichem Funktionsumfang für UC Smart und UC Suite verfügbar



Abbildung 2: 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 Systemstatistiken eingesetzt werden

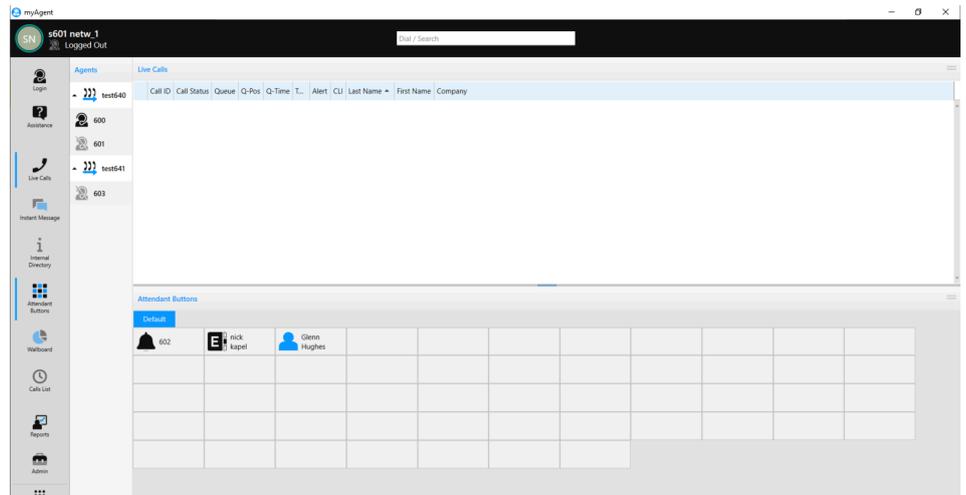


Abbildung 3: myAgent

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

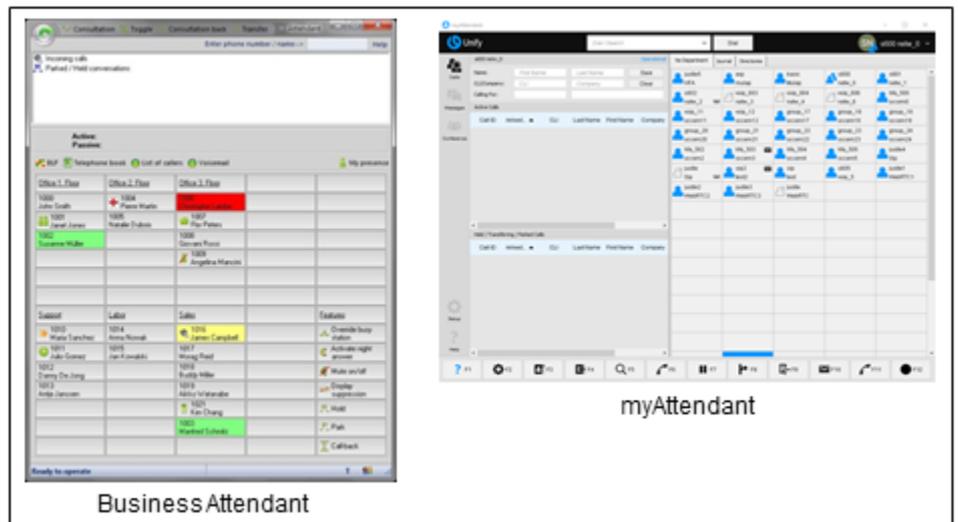


Abbildung 4: myAttendant

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 Gebührenausswertungen

Integrierte Services

- Directory Services für Informationen zu Anrufern und der Suche in internen und externen Verzeichnissen
- Präsenz-Management und IM (Instant Messaging) 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 in OpenScape Business integriert. UC Suite benötigt zusätzlich entweder die intern steckbare Baugruppe "UC Booster Card" oder den externen Linux-Server "UC Booster Server". Der Softswitch OpenScape Business S unterstützt wahlweise UC Smart oder UC Suite.

2.3.1 Vertriebliche Ausbaustufen

Die OpenScape Business Modelle haben unterschiedliche Ausbaustufen.

	X1	X3R/X3W	X5R/X5W	X8	S
Anbindung an Service-Provider					
ITSP-Kanäle (SIP-Provider)	30	60	60	60	180
Max. Anzahl aktiver SIP-Provider	8	8	8	8	8
ISDN S ₀ (BRI)	4	20	52	128	-
	via Mainboard	X3R: 2* STLSX4R X3W: 2* STLSX4	X5R: 6* STLSX4R X5W: 6* STLSX4	SW-Limit, d.h. unabhängig von der Anzahl der STDM3- Baugruppen	
ISDN S _{2M} (PRI)	-	30	30	120	-
			1* TS2	3 * DIUT3	
Max. Anzahl Leitungskanäle (ITSP, SIP-Q, Native SIP, TDM Leitungen, MEB)	250	250	250	250	250
Teilnehmer					
ISDN	4	20	52	128	-
	via Mainboard	X3R: 2* STLSX4R X3W: 2* STLSX4	X5R: 6* STLSX4R X5W: 6* STLSX4	8* STMD3	
Analog	4	20	52/68	384	-
	via Mainboard	X3R: 2* SLAV8R X3W: 1* SLAV16	X5R: 6* SLAV8R X5W: 4* SLAV16	16* SLMA	
Digital (U _{P0/E})	8	24	56	384	-
	via Mainboard	2* SLU8(R)	6* SLU8(R)	16* SLMO2	
IP-Teilnehmer	20 ¹	500	500	500	2000 (max. 500 SIP-Teilnehmer)
Cordless/DECT(CMI)	16	32	32/64	250	-
	1-7 Basisstationen via Mainboard	1-7 Basisstationen via Mainboard + 8-15 über SLUN	1-7 Basisstationen via Mainboard + 8-15 über SLUN	4* SLMUC	
Max. Anzahl Teilnehmer	30 ¹	500	500	500	2000
Unified Communications (UC Smart)					

Systemübersicht

	X1	X3R/X3W	X5R/X5W	X8	S
UC Smart VoiceMail (Smart VM)	30	500/320 ²	500/320 ²	500/320 ²	1500
Max. Anzahl gleichzeitig aktiver UC Smart Clients (Summe aus myPortal to go, Application Launcher, OpenScape Business Attendant, OpenScape Business BLF und WSI-Clients von Drittanbietern)	30	250/50 ²	250/50 ²	250/50 ²	250
OpenScape Business Attendant	8	8	8	8	8
OpenScape Business BLF	30	250	250	250	250
	Max. 350 BLF Tasten	Max. 350 BLF Tasten	Max. 350 BLF Tasten	Max. 350 BLF Tasten	Max. 350 BLF Tasten
Max. Anzahl der mobilen Teilnehmer	30	250/50 ²	250/50 ²	250/50 ²	250
Anzahl Mobility Entry User	30	150	150	150	250
myPortal to go	30	250/50 ²	250/50 ²	250/50 ²	250
myPortal for Teams	-	-	-	-	250
Max. Anzahl Kanäle für UC-Konferenzen	30	30	30	30	60
Unified Communications (UC Suite)					
UC Suite VoiceMail	-	500	500	500	1500
Max. Anzahl gleichzeitig aktiver UC Suite Clients (Summe aus myPortal for Desktop, myPortal for Outlook, myAttendant, myAgent)	-	500/150 ³	500/150 ³	500/150 ³	1500
Max. Anzahl weiterer gleichzeitig aktiver Clients (Summe aus myPortal to go, myPortal for Teams, Application Launcher, OpenScape Business Attendant, OpenScape Business BLF und 3rd Party WSI Clients)	-	-	-	-	500
myPortal for Desktop	-	500/150 ³	500/150 ³	500/150 ³	1500
myPortal for Outlook	-	500/150 ³	500/150 ³	500/150 ³	1500
myAttendant	-	20	20	20	20

	X1	X3R/X3W	X5R/X5W	X8	S
OpenScape Business Attendant	8	8	8	8	8
OpenScape Business BLF	30	250	250	250	500
	Max. 350 BLF Tasten	Max. 350 BLF Tasten	Max. 350 BLF Tasten	Max. 350 BLF Tasten	Max. 350 BLF Tasten
myAgent	-	192 einrichtbar / 64 parallel aktiv			
Max. Anzahl der mobilen Teilnehmer	-	250/150 ³	250/150 ³	250/150 ³	250
Anzahl Mobility Entry User	-	150	150	150	250
myPortal to go	-	250/100 ³	250/100 ³	250/100 ³	250
myPortal for Teams	-	-	-	-	250
myReports	-	1	1	1	1
Max. Anzahl gleichzeitiger Fax Kanäle	-	8	8	8	8
Max. Anzahl Fax User	-	500/150 ³	500/150 ³	500/150 ³	1500
Max. Anzahl Kanäle für UC-Konferenzen	-	20	20	20	60
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
TAPI 120/170 User (über CSTA, UC Booster Server/ Card notwendig)	-	500/150 ³	500/150 ³	500/150 ³	1500
TAPI 120 User (im UC Smart Modus via Mainboard ohne CSTA)	30	30	30	30	-
Directory Service Connector (UC Booster Card/Server notwendig)	-	4	4	4	4

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 / 2. Wert: Maximaler Ausbau mit UC Booster Card

³ 1. Wert: Maximaler Ausbau mit UC Booster Server / 2. Wert: Maximaler Ausbau mit UC Booster Card

Für eine detaillierte Beschreibung der Ausbaustufen/Ausbaugrenzen 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 (1500 Teilnehmer bei OpenScape Business S). 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 X1W
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.



Abbildung 5: 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 12 SP5 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

Systemübersicht

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 1000 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 12 SP5 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 <ul style="list-style-type: none"> • Nenneingangsspannung (AC): 100 bis 240 V • Nennfrequenz: 50/60 Hz • Batteriespeisung (DC): -48 V 					
Leistungsaufnahme	Abhängig von der Hardware-Plattform und dem Ausbau					
Umweltbedingungen	<ul style="list-style-type: none"> • 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))	<ul style="list-style-type: none"> • OpenStage 5/10/15/20/30/40/60/80
OpenScape Desk Phone (IP/HFA, SIP)	<ul style="list-style-type: none"> • OpenScape Desk Phone IP 35G/55G/35G Eco • OpenScape Desk Phone CP 100/200/205/400/600/600E/700/700X HFA und SIP • OpenScape Desk Phone CP 110/210/710 HFA und SIP
Beistellgeräte	<ul style="list-style-type: none"> • OpenStageKey Module nur für OpenStage 15/40/60 • OpenStage BLF 40 (Besetztlampenfeld) nur für OpenStage 40 und OpenStage 30 T • OpenScape Key Module 400/600, nur für CP 400/600/600E/700/700X • OpenScape Key Module 410/710, nur für CP 710
OpenScape Business Cordless	<ul style="list-style-type: none"> • OpenStage M3 • OpenScape DECT-Telefon S6/SL6/R6
PC-Clients (HFA, SIP)	<ul style="list-style-type: none"> • OpenScape Personal Edition (bei SIP inkl. Video)
SIP-Telefone (UC Suite) / AP-Adapter	<ul style="list-style-type: none"> • SIP-Telefone mit RFC 3725-Unterstützung • Mediatrix 4102S (zum Anschluss von 2 analogen Telefonen oder Faxgeräten)
WLAN-Telefone	<ul style="list-style-type: none"> • OpenStage WL3 professional • OpenScape WLAN-Telefon WL4/WL4 Plus
Analog- und ISDN-Telefone	<ul style="list-style-type: none"> • Analoge (a/b) Telefone • Digitale (S₀) ISDN-Telefone

Ältere Geräte (z. B. optiPoint 410/420/500, Gigaset M2/SL3/S4/SL4/S5 und 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.

Systemübersicht

Weiterführende Informationen

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.

Zugehörige Konzepte

[CSTA](#) auf Seite 661

2.4 Weiterführende Informationen

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

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	es	da	fi	ru	cs	pl	hr	hu	zh
	en	fr	no					tr		
		it	sv							
		nl								
		pt								
UC Smart Clients										
myPortal @work (Client)	X	X	X	X	X	X	X	-	-	-
myPortal @work (Benutzerhandbuch)	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	-	-	-
TUI (Telephone User Interface)	X	X	X	X	X	X	-	X	-	X
TUI (Kurzbedienungsanleitung)	X	X	-	-	-	-	-	-	-	-

	de en	es fr it nl pt	da no sv	fi	ru	cs	pl	hr tr	hu	zh
OpenScape Business Attendant / BLF (Client)	X	X	-	-	-	X	-	-	-	-
OpenScape Business Attendant / BLF (Bedienungsanleitung)	X	X	-	-	-	X	-	-	-	-
UC Suite Clients										
myPortal @work (Client)	X	X	X	X	X	X	X	-	-	-
myPortal @work (Benutzerhandbuch)	X	X	X	X	X	X	X	-	-	-
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 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	-	-	-
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	-	-	-

Systemübersicht

	de en	es fr it nl pt	da no sv	fi	ru	cs	pl	hr tr	hu	zh
Manager E (Administratordokumentation/Online/ Hilfe)	X	X	-	-	X	-	-	-	-	-

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

Tipp: 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>

Administrationskonzept

OpenScape Business Assistant (WBM)

3 Administrationskonzept

Die Administration des Kommunikationssystems erfolgt mit dem OpenScape Business Assistant.

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 Administratorprofil.

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.

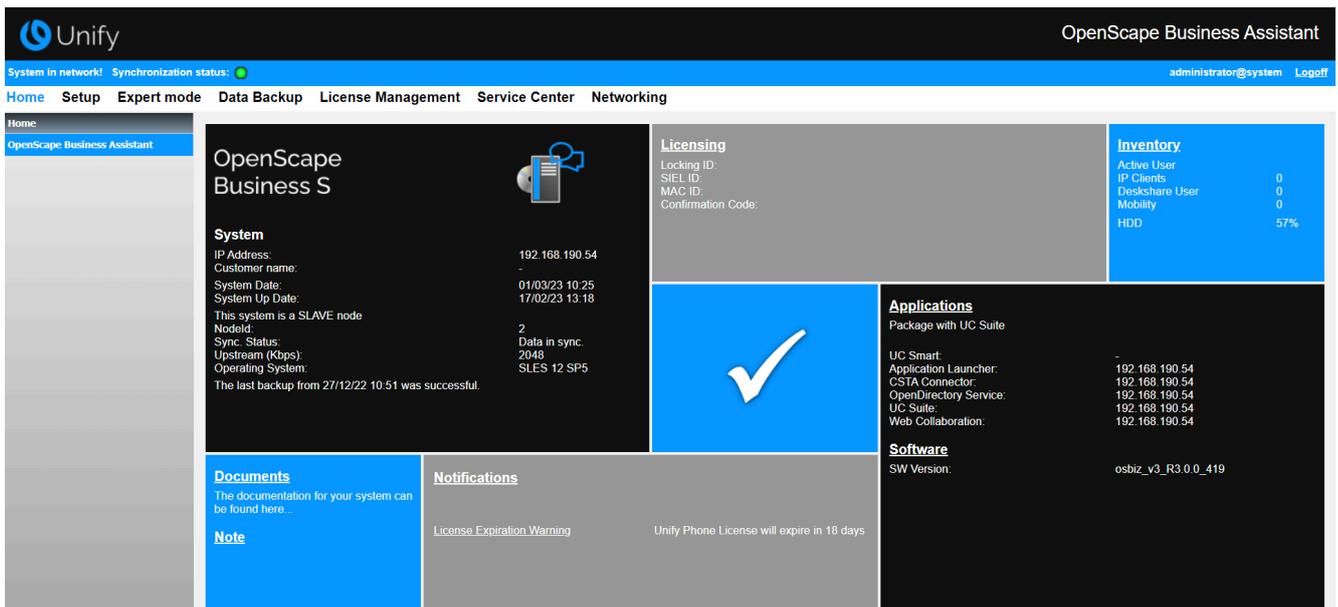
Unterstützte Webbrowser:

- Microsoft Internet Explorer 10 oder neuer
- Microsoft Edge
- Mozilla Firefox 18 oder neuer
- Google Chrome

3.1.2 Startseite des WBM

Auf der Startseite des WBM werden wichtige Systeminformationen angezeigt, die in verschiedene Bereiche (Kacheln) aufgeteilt sind. Zusätzlich gibt sie Hinweise und informiert über Systemfehler, Ereignisse und Aktionen.

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



Die folgenden Informationen werden angezeigt:

- Bereich: **Status** (Mitte)
 - Weißes Häkchen auf blauem Hintergrund: das Kommunikationssystem ist voll funktionsfähig - rot hinterlegte Meldungen in den anderen Feldern weisen auf Aktionen hin, die durchgeführt werden sollten.
 - Weißes Ausrufezeichen 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
 - Datum und Uhrzeit aktuell
 - Datum und Uhrzeit des letzten Neustarts des Systems
 - Hinweise beim Betrieb in einem Netzverbund (System ist Master oder Slave, Anzeige der Knoten-ID)
 - Synchronisationsstatus
 - Upstream-Bandbreite in Kbit/s
 - SDHC-Integritätsstatus
 - Hinweise für Sichern und Wiederherstellen
 - Status der Booster-Karte
- Bereich: **Dokumente**
 - Link zur Dokumentation
- Bereich: **Benachrichtigungen**
 - Verschiedene Benachrichtigungen über das System
- Bereich: **Hinweis**
 - Zeigt die von einem Administrator zuletzt eingegebenen Informationen an. Durch Klicken auf die unterstrichene Überschrift wird ein Textfenster geöffnet, in dem alle

Administrationskonzept

Informationen angezeigt und weitere Informationen eingegeben werden können.

Daten des Notizfelds sind nicht im Backup-Set des Systems enthalten. Daher werden diese Daten beim Wiederherstellen eines Backup-Sets nicht wiederhergestellt.

- Bereich: **Lizenzierung**
 - Locking-ID für die Lizenzierung
 - SIEL-ID für die Lizenzierung
 - Hinweis auf den Lizenzierungsstatus, der angibt, ob das System sich im Lizenzmodus "Permanent" oder "Pay As You Go" (PAYG) befindet.
- Bereich: **Inventory**
 - Typ und Anzahl der aktiven Teilnehmer
 - Anzahl der aktivierten ITSPs und Link zum ITSP-Status-Dialog im Service-Center der aktiven Teilnehmer
- Bereich: **Applikationen** und Software
Applikationen:
 - Verwendetes Applikationspaket (UC Smart oder UC Suite) und dessen Komponenten inkl. der IP-Adressen der verwendeten Server.
 - Gibt an, ob eine UC Booster Card gesteckt ist.Software:
 - Version der installierten Software des Kommunikationssystems
 - Gibt an, 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.
 - Ablaufdatum des 3-jährigen Software-Supports.Nach dem Ablaufdatum erscheint die Meldung "Die Software-Support-Lizenz ist abgelaufen. Bitte aktualisieren Sie Ihre Software-Support-Lizenz".
 - Hinweis auf neue Softwareversion

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 erscheint an oberster Stelle der Name des gewählten Aufgaben-Centers. 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.

3.1.4 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. Auch das Passwort eines Manager E-Administrators kann geändert werden.

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. Für ein sicheres Passwort sollte zusätzlich mind. ein Großbuchstabe, ein Kleinbuchstabe und ein Sonderzeichen enthalten sein.

Profile

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

Um zu verhindern, dass sich ein böswilliger Benutzer über ISDN einloggt und das Default-Passwort bei der Erstanmeldung ändert, muss der Benutzer das Passwort über Manager E in einem separaten Schritt bei der Installation zwingend ändern.

Anmerkung: Ein Passwort, das aus 5 Sternen (*****
besteht, wird aus Sicherheitsgründen vom System nicht
akzeptiert.

Tabelle 1: Profil-Berechtigungen

Profil	Berechtigung
<p>Basic geringe Kenntnisse im Konfigurieren des Systems</p>	<p>Systeminformationen auf der Startseite</p> <p>Wizard Tastenprogrammierung</p> <p>Wizard Telefonbuch / Kurzwahl</p> <p>Wizard Gesprächsdatenerfassung</p> <p>Wizard Wartemusik / Ansagen</p> <p>Wizard Teilnehmername und Freischaltung</p> <p>Zugriff auf Administratoren (nur Änderung des eigenen Passworts)</p> <p>Zugriff auf Lizenzverwaltung > Lizenzinformationen</p> <p>Zugriff auf Service-Center > Dokumente</p> <p>Zugriff auf Service-Center > Software</p>
<p>Enhanced Gute Kenntnisse im Konfigurieren des Systems</p>	<p>Wie das Profil Basic, plus:</p> <p>Zugriff auf alle Wizards (außer Grundinstallation, UC Suite und UC Smart)</p> <hr/> <p>Anmerkung: In OpenScape Business S Systemen wird der Zugriff auf alle Wizards nicht unterstützt.</p> <hr/> <p>Zugriff auf Administratoren (nur Änderung des eigenen Passworts)</p> <p>Zugriff auf Sicherung und Wiederherstellung</p> <p>Zugriff auf Lizenzverwaltung (ohne Registrierung, Lizenzaktivierung und Einstellungen)</p> <p>Zugriff auf Service-Center > Inventory</p> <p>Zugriff auf Service-Center > Restart / Reload (ohne Reload)</p> <p>Zugriff auf Service-Center > Diagnose > Status</p> <p>Zugriff auf Service-Center > Diagnose > Event Viewer</p>

Profil	Berechtigung
Advanced Geschulte Benutzer	Wie das Profil Enhanced , plus: Zugriff auf alle Wizards Zugriff auf Administratoren (nur Änderung des eigenen Passworts) Zugriff auf die komplette Lizenzverwaltung Zugriff auf das komplette Service-Center Zugriff auf Networking
Expert Geschulte Servicetechniker	Wie das Profil Advanced , plus: Zugriff auf Administratoren (vollständig) Zugriff auf den Experten-Modus

Tabelle 2: Profil-Verwaltung

Profil	Wartung
Basic geringe Kenntnisse im Konfigurieren des Systems	Kann eigenes Passwort ändern. Sieht außer sich selbst keine weiteren konfigurierten Administratoren.
Enhanced Gute Kenntnisse im Konfigurieren des Systems	Kann eigenes Passwort ändern. Sieht außer sich selbst keine weiteren konfigurierten Administratoren.
Advanced Geschulte Benutzer	Kann eigenes Passwort ändern. Sieht außer sich selbst keine weiteren konfigurierten Administratoren.
Expert Geschulte Servicetechniker	Kann eigenes Passwort und die Benutzernamen und Passwörter anderer Administratoren ändern. Sieht alle konfigurierten Administratoren. Kann Administratoren hinzufügen, bearbeiten und entfernen.

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

Administrator-Verwaltung im Netzverbund

Die direkte Verwaltung der Administratoren ist nur im WBM des Master-Knotens möglich. An Slave-Knoten wird das Menü **Administrator** nicht angezeigt. Alle Administrator-Konfigurationen werden an die Slave-Knoten übertragen. Es ist aber möglich, im WBM des Slave-Knotens über die Knotenansicht das WBM des Master-Knotens aufzurufen. Hier wird das Menü **Administrator** angezeigt und die Administratoren können verwaltet werden.

Anmerkung: Das Hinzufügen/Bearbeiten/Löschen von Benutzern kann nicht über einen WBM-Zugang im Slave-Modus (sondern nur über WBM-Zugang im Master-Modus) erfolgen.

Verwaltung des Manager E-Passworts

Ein Administrator kann das Passwort der Benutzer ändern (aber keine neue Benutzerrolle erstellen), die über Manager E auf das integrierte System zugreifen können.

Nur bereits vorhandene Benutzer werden aufgefordert, das Passwort zu ändern. Die Benutzergruppe sowie Optionen wie „Erstellt“, „Zuletzt verwendet“ können jedoch nicht geändert werden und werden nicht angezeigt. Dies ist eine Sicherheitsfunktion, weshalb nicht der gesamte Administratorbildschirm von Manager E angezeigt wird.

3.1.5 Wizards

Kundenadministrator (Profil Basic) steht ein ausgewählter Teil der Wizards zur Verfügung. 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**

Administrationskonzept

Einmalige Nutzung bei Ersteinrichtung. Länderinitialisierung, 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**

Zugangparameter 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**
Zugangsparameter des Internet-Telefonie Service Provider (ITSP) z.B. Benutzerkonto, 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 (Türöffner)**
Einrichtung von Rufzuordnung und Zugriffsberechtigung der Türsprechstelle am analogen Teilnehmeranschluss.
- **SmartVM**
Einrichtung der UC Smart Sprachbox (SmartVM).
- **Blacklist für eingehende Anrufe**
Sie können eine Liste mit Nummern erstellen, um unerwünschte Anrufer dauerhaft zu blockieren.
- **Active Directory Integration Service**
Active Directory einrichten

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 Codeschlusses für einzelne Teilnehmer.

- **Gruppenruf / Sammelanschluss**

Einrichtung von kommenden Anrufen für Teilnehmergruppen (parallele, lineare oder zyklischen Rufreihenfolge).

- **Anrufumleitung**

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.

- **UCD**

Einrichtung einer automatischen intelligenter Anrufverteilung auf eine Gruppe mit ausgewählten Teilnehmer.

- **Vermittlungsplatz**

Einrichtung von Teilnehmern als Vermittlungsplatzzrufnummer 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.
- **Abteilungen**
Konfiguration von Abteilungen.
- **Gruppen**
Konfiguration von Voicemail- und Fax-Gruppen.
- **Templates**
Konfiguration von SMS-Templates.
- **Externes Verzeichnis**
Manuelles Hinzufügen einzelner Kontakte zum externen Verzeichnis.
- **Konfiguration externe 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.
- **Konferenz**
Konfiguration von Konferenzschaltungen.
- **Profile**
Erstellen von Benutzer-Profilen.
- **Faxkopfzeilen**
Konfiguration von Faxkopfzeilen.
- **Skin-Einstellungen**
Verwaltung von Benutzer-Oberflächen.

3.1.5.9 Assistenten – Circuit

Die Assistenten unter **Circuit** unterstützen die Verwendung von Circuit-Funktionen.

Folgende Assistenten sind unter **Circuit** verfügbar:

- **Circuit-Anbindung**
Konfiguration der Grundeinstellungen für Circuit einschließlich HUTC.
- **Circuit-Benutzerinstanz**
Konfigurieren Sie die Circuit-Benutzerinstanz.

3.1.5.10 Assistenten – Globales Verzeichnis

Die Assistenten unter **Globales Verzeichnis** unterstützen das Importieren und Bearbeiten von Verzeichniskontakten.

Folgende Assistenten sind unter **Globales Verzeichnis** verfügbar:

- **Kontakte importieren**
Der Assistent führt Sie durch den Import von Kontaktdaten aus CSV in das globale Verzeichnis.
- **Kontakte bearbeiten**
Sie können manuelle Einträge im globalen Verzeichnis hinzufügen oder bearbeiten.

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

Die Option **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 Sma	UC Suite
Administratorokumentationen (PDF)	-	x
Bedienungsanleitungen (PDF)	-	x
Links zu weiterführenden Informationen	x	x

Inhalt	UC Sma	UC Suite
CSV-Vorlagen für den Import von Daten für <ul style="list-style-type: none"> • Teilnehmer • Kurzwahl zentral KWZ • Externes Verzeichnis 	x	x

Zugehörige Konzepte

[Accounting-Tools](#) auf Seite 697

3.1.6.2 Service Center – Software

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

Folgende Inhalte sind verfügbar:

Inhalt	UC Sma	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 > System

System gibt einen Überblick über grundlegende Konfigurationsdaten des Systems.

3.1.6.4 Service Center – Inventory > Rufnummern

Rufnummern stellt eine Liste aller zugeordneten Rufnummern zur Verfügung.

3.1.6.5 Service Center – Inventory > Netzwerkübersicht

Netzwerkübersicht bietet eine Liste mit Informationen über die aktuell im Netzwerk befindlichen Systeme.

3.1.6.6 Service-Center – Software-Update

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

3.1.6.7 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.

3.1.6.8 Service-Center – Remote-Zugang

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

3.1.6.9 Service-Center – Restart / Reload

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

3.1.6.10 Service-Center – Diagnose > Status

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

Siehe auch [Inventory-Management](#) .

3.1.6.11 Service-Center – Diagnose > Event Viewer

Event Viewer protokolliert Systemereignisse.

Siehe auch [Traces](#) .

3.1.6.12 Service-Center – Diagnose > Trace

Trace bietet Möglichkeiten zur Fehlerprotokollierung.

Siehe auch [Traces](#) .

3.1.6.13 Service-Center – Diagnose > Service-Protokoll

Im Service-Protokoll werden verschiedene Systemdaten in Form von HiPath 3000-Ereignissen protokolliert.

Sie müssen sich im WBM-Ansichtsmodus befinden, um die Datei zu aktualisieren oder herunterzuladen.

3.1.7 Experten-Modus

Der Experten-Modus stellt geschulten Servicetechnikern (Profil **Experten**) 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
- **Suche**
bietet eine Volltextsuche zum gezielten Auffinden relevanter Themen

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 X1, OpenScape Business X3, OpenScape Business X5 und OpenScape Business X8. Die OpenScape Business S ist nicht mit dem Manager E administrierbar.

Es ist ratsam, Konfigurationsänderungen nur dann über Manager E vorzunehmen, wenn Sie nicht über WBM vorgenommen werden können, wie beispielsweise die Dämpfung, Klingelimpuls, Tonfrequenz usw. Änderungen, die über Manager E vorgenommen werden, müssen über den Deltamodus abgesendet werden.

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

Administrationskonzept

- 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 Bedienoberfläche von Assistant T.

Folgende Leistungsmerkmale sind nicht mehr über Manager E administrierbar:

- Lizenzierung
- Netzwerk
 - SNMP-Partner
 - PSTN-Partner
 - Routing
 - Mapping
 - Gatekeeper
 - Durchw. H.323
 - IP-Ports
- Wartung
 - Error History
 - Event-Protokoll
 - 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

4 Ersteinrichtung von OpenScape Business X

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

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

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

Voraussetzung für die Ersteinrichtung 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
- Teilnehmerkonfiguration
- Lizenzierung
- Systemhärtung
- 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 usw.) und der vorhandenen Infrastruktur gelten folgende allgemeine Voraussetzungen:

- Die Infrastruktur (LAN, TDM-Telefonnetz) ist vorhanden und nutzbar.

Ersteinrichtung von OpenScape Business X

- 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-S₀- 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:

- Netzwerkschnittstelle:

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
- Microsoft Edge
- Mozilla Firefox ab Version 17.
- Google Chrome

Falls eine ältere Webbrowser-Version installiert ist, muss eine aktuelle Version installiert werden, bevor mit der Erstinbetriebnahme begonnen werden kann.

- Java:

Es muss Oracle Java Version 8 oder höher bzw. OpenJDK 8 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

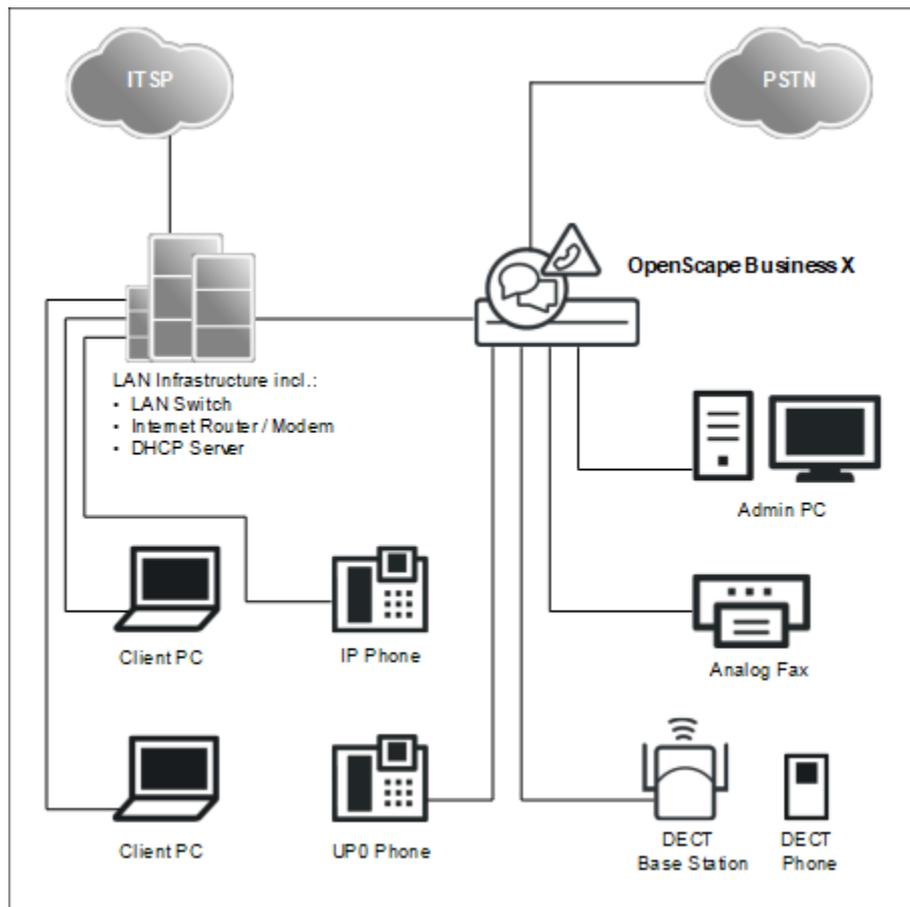
Die analogen Teilnehmer (z.B. analoges FAX) sind direkt am Kommunikationssystem angeschlossen.

- 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).

Ersteinrichtung von OpenScape Business X
Rufnummernplan



4.3 Rufnummernplan

Ein Rufnummernplan ist eine Liste aller im Kommunikationssystem verfügbaren Rufnummern. Er beinhaltet u.a. interne Rufnummern, Durchwahlrufnummern 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):	0 = Welt / 9 = USA	0 = Welt / 9 = USA
Rtg. 1 (Amt ISDN, analog)	-	851
Rtg. 8 (UC Suite)	Nicht vorbelegt	855-858
Rtg. 12-15 (Amt ITSP)	Nicht vorbelegt	859
Rtg. 16 (Vernetzung)		
Rufnummer für den Remote-Zugang	Nicht vorbelegt	Nicht vorbelegt
Rufnummer für Sprachnachrichten	351	351
UC Smart	-	Nicht vorbelegt
UC Suite		

Individueller Rufnummernplan

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

Die XML-Datei enthält mehrere Register. Das Register "Kunde" 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 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
192.168.1.3	Application Board (optional)
192.168.1.10	E-Mail-Server

Ersteinrichtung von OpenScape Business X

IP-Adressbereich	Clients
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 (überholt)
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 OpenScope 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 Kommunikationssystem ins interne LAN integriert werden.

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



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



GEFAHR: Das Einschalten von OpenScope 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 OpenScope Business X1W/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.

4.6 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 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 des Kommunikationssystems (siehe auch [IP-Adressen-Schema](#)).

4.6.2 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 \(DLS und DLI\)](#)). 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 \(DLS und DLI\)](#)).

- 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.

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

4.6.3 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

- Wie Sie das Datum und die 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.

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

- Wie Sie das Datum und die 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 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 OpenScape Business X Mainboard intergiert.

- **Paket mit UC Suite**

Die UC-Lösung UC Suite ist auf der zusätzlich intern steckbaren Baugruppe "UC Booster Card" intergiert.

- **Paket mit UC Suite auf OSBiz UC Booster-Server**

Die UC-Lösung UC Smart ist auf dem externen Linux-Server "OpenScape Business UC Booster Server" 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 Anschluss des Kommunikationssystems ans Kunden-LAN

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

4.7 Basiskonfiguration

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

Der Wizard Basisinstallation beinhaltet einen Progress Indicator, der den aktuellen Schritt sowie die darauf folgenden Schritte anzeigt.

4.7.1 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 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 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.

Anmerkung:

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:

- 1) Teilnehmerdaten anzeigen**

Sie können sich alle vorkonfigurierten Rufnummern und Teilnehmerdaten anzeigen lassen.

- 2) Alle Rufnummern löschen (optional)**

Verwenden Sie einen individuellen Rufnummernplan, müssen Sie alle vorkonfigurierten Rufnummern löschen.

- 3) Vorkonfigurierte Rufnummern an den individuellen Rufnummernplan anpassen (optional)**

Verwenden Sie einen individuellen Rufnummernplan, können Sie die vorkonfigurierten Rufnummern an den eigenen Rufnummernplan anpassen.

Anmerkung:

Geht der Benutzer die Option **Vorkonfigurierte Rufnummern ändern** durch, muss eine bereits in UC Suite vorhandene, benutzerdefinierte Konfiguration geändert oder wiederholt werden (z.B. Pilot-Warteschlangen)

- 4) 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:

- 1) 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.

- 2) 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 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 S₀-Schnittstellen zur Verfügung.

Sie haben folgende Möglichkeiten:

- ISDN-Konfiguration aktivieren:
 - 1) ISDN-Anlagenanschluss konfigurieren**

Sie können einen ISDN-Amtsanschluss als Anlagenanschluss mit Durchwahlnummern einrichten.
 - 2) ISDN-Mehrgeräteanschluss konfigurieren**

Sie können einen ISDN-Amtsanschluss als Mehrgeräteanschluss mit MSN einrichten.
 - 3) Anschluss von ISDN-Teilnehmern konfigurieren (optional)**

Eine oder mehrere S₀-Schnittstellen können als interne S₀-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 S₀-Schnittstellen werden automatisch als interne S₀-Anschlüsse konfiguriert.

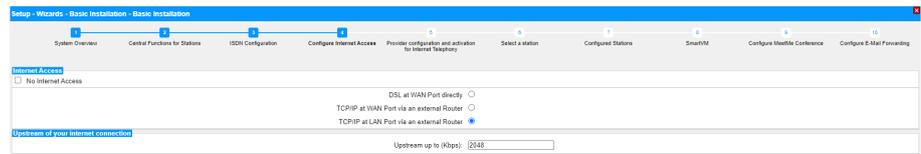
Weitere Möglichkeiten für einen Amtsanschluss

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 Internetzugang

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

Ersteinrichtung von OpenScape Business X



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)

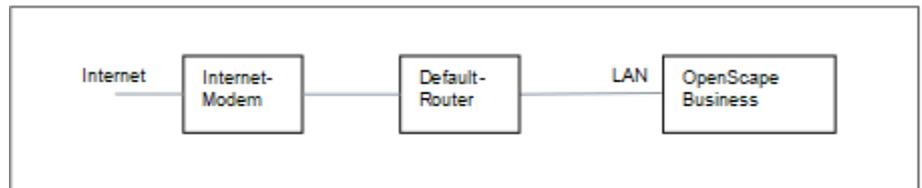


Dazu nutzen Sie den WAN-Anschluss des Kommunikationssystems. OpenScape Business kennt entweder den Internet-Router oder arbeitet als DHCP-Client. Diese Möglichkeit kann verwendet werden, wenn der Internet-Router

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 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 8 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.

Anmerkung:

Einrichtebeispiele finden Sie im Internet im **Unify Experts Wiki** unter *OpenScape Business - SIP / ITSP Connectivity - PDF "OSBiz V2 Configuration for ITSP"*.

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 Bereich werden dann manuell als interne Rufnummern der Teilnehmer vergeben.

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	Durchwahl
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 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 S₀-Schnittstelle als internen S₀-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 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-Teilnehmer sind z.B. LAN-Telefone oder WLAN-Telefone.

4.7.7 Konfiguration von UC Suite

Im Fenster **Automatische Konfiguration der Applikation-Suite** können Sie die automatische Konfiguration der UC-Lösung UC Suite durchführen.

Anmerkung: Dieses Fenster erscheint nur, wenn im Wizard **Erstinstallation** bei der Applikationsauswahl **Paket mit UC Suite** gewählt wurde.

Die automatische Konfiguration der UC-Lösung UC Suite erfordert eine Anzahl von freien Amtsleitungen, die für die Anwendung statisch belegt werden. Diese Anzahl hängt von den Kapazitäten der Systemspezifikation ab und ist im Abschnitt [Maximalwerte für Leitungen](#) auf Seite 835 aufgeführt (siehe *MEB-Leitungskanäle für UC Suite* in den Tabellen). Falls die Gesamtgrenze von 250 Leitungen überschritten wird, ist die Konfiguration der UC Suite nicht möglich.

4.7.8 Konfiguration der UC Smart Sprachboxen

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.

Anmerkung:

Dieses Fenster erscheint nur, wenn im Wizard **Erstinstallation** bei der Applikationsauswahl **Paket mit UC Smart** gewählt wurde.

4.7.9 Konferenz-Server-Einstellungen

Im Fenster **MeetMe-Konferenz-Einstellungen ändern** können Sie die Rufnummer und die Einwahlnummer für Konferenzen festlegen.

4.7.10 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.

Anmerkung: 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.

4.8 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) 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.

2) UC Smart Client zur Installation bereitstellen (nur für UC Smart)

3) Wie Sie UC Suite Clients zur Installation bereitstellen (nur für UC Suite)

Die UC Suite Clients sind Bestandteil von 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. Weitere Informationen finden Sie unter [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.

4.9 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.

Anmerkung: 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 eingetragen 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 eingetragen 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 eingetragen 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 Ersteinrichtung von OpenScape Business S

Beschrieben wird die Ersteinrichtung von OpenScape Business S (kurz Softswitch genannt). Der Softswitch und die zugehörigen 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 12 SP5 64 Bit die OpenScape Business Kommunikationssoftware installiert. Die Kommunikationssoftware kann direkt auf einem Linux-Server oder in einer virtuellen Umgebung mit VMware vSphere oder Microsoft Hyper-V betrieben werden. Die Installation des Linux-Betriebssystems ist beschrieben in der Installationsanleitung *OpenScape Business, Installation Linux Server*.

Die Ersteinrichtung 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 Ersteinrichtung 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 Ersteinrichtung hinausgehenden Leistungsmerkmale finden Sie in den anschließenden Kapiteln.

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

Übersicht über die wichtigsten Installationsschritte:

- Systemeinstellungen
- Systemrufnummern und Vernetzung
- Internet-Telefonie
- Teilnehmerkonfiguration
- Lizenzierung
- Systemhärtung
- Datensicherung

5.1 Voraussetzungen für die Ersteinrichtung

Die Erfüllung der Voraussetzungen für die Ersteinrichtung gewährleistet den Betrieb von OpenScape Business S.

Allgemeines

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

- Die LAN-Infrastruktur (Internet-Router, Switches, usw.) ist vorhanden und nutzbar.

Ersteinrichtung von OpenScape Business S

- Die IP-Telefone sind an das Kunden-LAN angeschlossen.
- Der für OpenScape Business S benötigte Linux-Server wurde nach der *OpenScape Business 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, 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 OpenScape Business Kommunikationssoftware. Diese DVD bzw. ISO-Datei ist im Lieferumfang enthalten.
- DVD mit Linux-Betriebssystem SLES SLES 12 SP5
Die Linux-DVD wird ggf. bei der Installation der OpenScape Business Kommunikationssoftware benötigt, da einige der erforderlichen Software-Pakete (RPM) später über die DVD bzw. die ISO-Datei nachinstalliert werden müssen.

Administration

Für die Ersteinrichtung 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 11 (Admin-PC)
 - Microsoft Edge
 - Mozilla Firefox Version 37.x und 38.x
 - Mozilla Firefox ESR Version 24.x und 31.x
 - Google ChromeFalls eine ältere Webbrowser-Version installiert ist, muss eine aktuelle Version installiert werden, bevor mit der Ersteinrichtung des Systems begonnen werden kann.
- Java:
Es muss Oracle Java Version 8 oder höher bzw. OpenJDK 8 installiert sein. Ist eine ältere Version installiert, muss auf die aktuellste Version aktualisiert werden, bevor mit der Ersteinrichtung 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](#)).

Internetzugang

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 to go
- Remote Service

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 Ersteinrichtung 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

Ersteinrichtung von OpenScape Business S

Komponenten

virtuellen Umgebung betrieben, so muss dem virtuellen System ebenfalls 4 GB RAM zugewiesen werden.

5.2 Komponenten

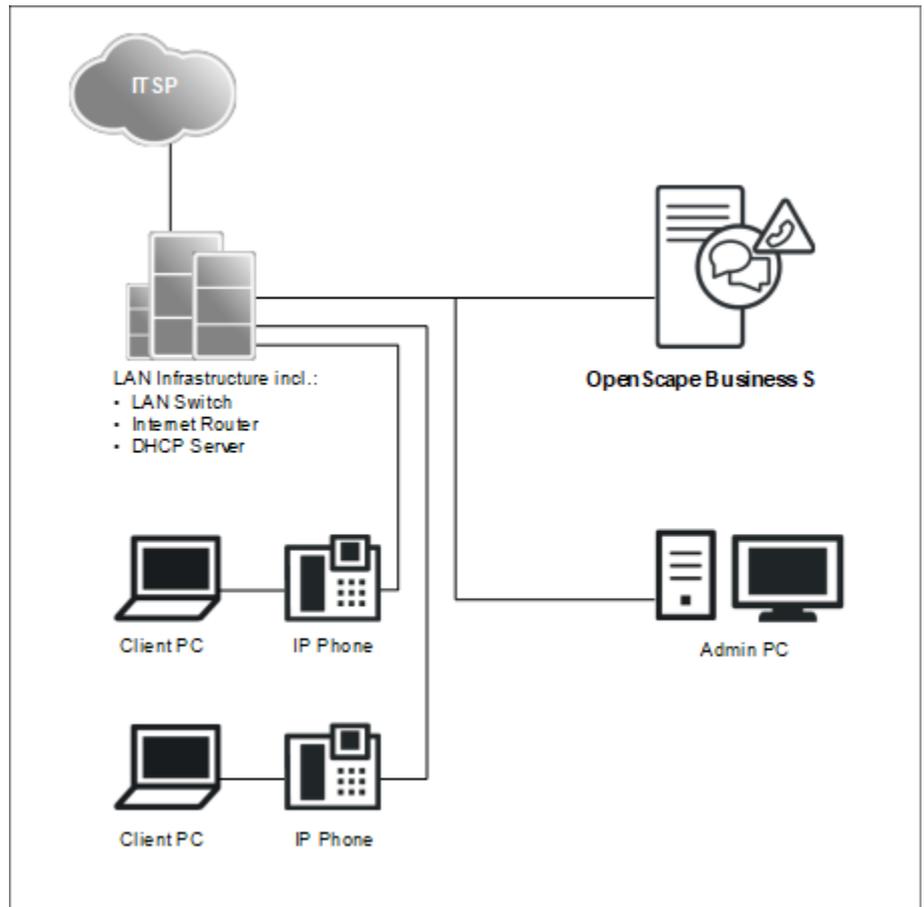
Die Komponenten des Installationsbeispiels sind im Folgenden beschrieben und skizziert.

Das Installationsbeispiel umfasst folgende Komponenten:

- OpenScape Business S
Der Linux-Server mit der OpenScape Business S Kommunikationssoftware wird über seine LAN-Schnittstelle in das vorhandene Kunden-LAN eingebunden.
- Admin-PC
Der Admin-PC wird 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
192.168.1.50 bis 192.168.1.254	Client-PCs & IP-Telefone, zugleich IP-Adressband des DHCP-Servers, Zuweisung der IP-Adressen an die Clients erfolgt dynamisch

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
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 "Kunde" 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.

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 externe 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 oder .ISO-Datei installiert (siehe hierzu *OpenScape Business Linux Server Installationsanleitung*).

- Gemeinsame Installation von Linux und Kommunikationssoftware (nur VMWare)

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), das 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 100 GB (50 bis 100 Benutzer) oder 200 GB (bis 500 Benutzer oder bei OpenScape Business Contact Center) oder 500 GB (über 500 Benutzer) angepasst werden.

Für Linux-Updates benötigen Sie zusätzlich den OpenScape Business 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>).

Alle Informationen über Schnappschüsse in Microsoft Hyper-V sind über die Microsoft Technet-Bibliothek unter technet.microsoft.com, Kapitel Hyper-V abrufbar.

5.6 Inbetriebnahme

Mit dem Wizard **Erstinstallation** des WBM werden die grundlegenden Einstellungen durchgeführt.

5.6.1 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.

5.6.2 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 in OpenScape Business S integriert.

- **Paket mit UC Suite**

Die UC-Lösung UC Suite ist in OpenScape Business S integriert.

5.7 Basiskonfiguration

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

Der Wizard Basisinstallation beinhaltet einen Progress Indicator, der den aktuellen Schritt sowie die darauf folgenden Schritte anzeigt.

5.7.1 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 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.

5.7.2 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.

Anmerkung:

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:

1) Teilnehmerdaten anzeigen

Sie können sich alle vorkonfigurierten Rufnummern und Teilnehmerdaten anzeigen lassen.

2) Alle Rufnummern löschen (optional)

Verwenden Sie einen individuellen Rufnummernplan, müssen Sie alle vorkonfigurierten Rufnummern löschen.

3) Vorkonfigurierte Rufnummern an den individuellen Rufnummernplan anpassen (optional)

Verwenden Sie einen individuellen Rufnummernplan, können Sie die vorkonfigurierten Rufnummern an den eigenen Rufnummernplan anpassen.

Anmerkung:

Geht der Benutzer die Option **Vorkonfigurierte Rufnummern ändern** durch, muss eine bereits in UC Suite vorhandene, benutzerdefinierte Konfiguration geändert oder wiederholt werden (z.B. Pilot-Warteschlangen)

4) 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:

1) 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.

2) 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.

5.7.3 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 8 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.

Anmerkung:

Einrichtebeispiele finden Sie im Internet im **Unify Experts Wiki** unter *OpenScape Business - SIP / ITSP Connectivity - PDF "OSBiz V2 Configuration for ITSP"*.

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 Bereich werden dann manuell als interne Rufnummern der Teilnehmer vergeben.

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	Durchwahl
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).

5.7.4 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.

5.7.5 Konfiguration von UC Suite

Im Fenster **Automatische Konfiguration der Applikation-Suite** können Sie die automatische Konfiguration der UC-Lösung UC Suite durchführen.

Anmerkung: Dieses Fenster erscheint nur, wenn im Wizard **Erstinstallation** bei der Applikationsauswahl **Paket mit UC Suite** gewählt wurde.

5.7.6 Konfiguration der UC Smart Sprachboxen

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.

Anmerkung:
Dieses Fenster erscheint nur, wenn im Wizard **Erstinstallation** bei der Applikationsauswahl **Paket mit UC Smart** gewählt wurde.

5.7.7 Konferenz-Server-Einstellungen

Im Fenster **MeetMe-Konferenz-Einstellungen ändern** können Sie die Rufnummer und die Einwahlnummer für Konferenzen festlegen.

5.7.8 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.

Anmerkung: 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 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) 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.

2) UC Smart Client zur Installation bereitstellen (nur für UC Smart)

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. Weitere Informationen finden Sie unter [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 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.

Anmerkung: 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 eingetragen 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 eingetragen 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 Deinstallation der Kommunikationssoftware

Die Deinstallation der Kommunikationssoftware ist über eine Text-Konsole möglich.

5.11 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.

Eine aktuelle und vollständige Liste aller verwendeten Ports von OpenScape Business finden Sie in der „Interface Management Database“ (IFMD), die über das Partnerportal von Unify (<https://unify.com/en/partners/partner-portal>) zugänglich ist.

Anmerkung: Die in der folgenden Liste mit „O“ gekennzeichneten Ports sind optional, d. h. sie sind in der Firewall nicht permanent geöffnet.

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
CLS	X		7780	O		O	
			7790				

Ersteinrichtung von OpenScape Business S

Beschreibung	TCP	UDP	Portnummer	OpenScape Business X	UC Booster Card	OpenScape Business S	UC Booster Server
Communication Client-Installationsprogramm	X		8101	X	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	
HFA	X		4060	X		X	
HFA Secure	X		4061	X		X	
Instant Messaging (http)	X		8101	X	X	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
xNAT traversal (NAT-T)		X	4500	X			
NTP		X	123	X			
xOpenfire Admin (https)	X		9091		X	X	X
OpenScape Business Auto Update Service (http)	X		8101	X	X	X	X
OpenScape Business Multisite	X		8778		X	X	X
OpenScape Business myReports (http)	X		8101		X	X	X
OpenScape Business Status Server	X		8808	X		X	X

Ersteinrichtung von OpenScape Business S

Beschreibung	TCP	UDP	Portnummer	OpenScape Business X	UC Booster Card	OpenScape Business S	UC Booster Server
OpenScape Business Benutzerportal	X	X	8779		X	X	X
Postgres	X		5432	X	X	X	X
RTP (eingebettet)		X	29100-30530	X	X	X	X
RTP (Server)		X	29100-30888	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	
VSL	X		8770-8780		X	X	X
Webadmin for Clients	X		8803	X	X	X	X
Webbased Clients							
Webbased Clients (http)	X		8801	X	X	X	X
Webbased Clients (https)	X		8802	X	X	X	X

Anmerkung: 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 Ersteinrichtung 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 Ersteinrichtung 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 Ersteinrichtung hinausgehenden Leistungsmerkmale finden Sie in den anschließenden Kapiteln.

Ersteinrichtung OpenScape Business UC Booster Card

Die OpenScape Business UC Booster Card wird in das OpenScape Business Kommunikationssystem X3/X5/X8 montiert und für den Betrieb konfiguriert. Anschließend wird die Konfiguration der OpenScape Business UC Booster Funktionalität durchgeführt.

Die Ersteinrichtung 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
<p>Montage der UC Booster Card</p> <p>Die UC Booster Card wird in das OpenScape Business Kommunikationssystem X3/X5/X8 montiert.</p> <p>Beschreibung siehe OpenScape Business Servicedokumentation, Montage der Hardware - Beschreibung der Baugruppen.</p>	<p>Montage der UC Booster Card</p> <p>Die UC Booster Card wird in das OpenScape Business Kommunikationssystem X3/X5/X8 montiert.</p> <p>Beschreibung siehe OpenScape Business Servicedokumentation, Montage der Hardware - Beschreibung der Baugruppen.</p>

Ersteinrichtung OpenScape Business UC Booster

Integration in neues Kommunikationssystem	Integration in bestehendes Kommunikationssystem
<p>Konfiguration der UC Booster Card</p> <p>Die Konfiguration der UC Booster Card wird zusammen mit der Erstinstallation des OpenScape Business Kommunikationssystems X3/X5/X8 durchgeführt.</p> <p>Beschreibung siehe Integration ins Kunden-LAN.</p>	<p>Konfiguration der UC Booster Card</p> <p>Die Konfiguration der UC Booster Card wird nachträglich an einem bereits konfigurierten OpenScape Business Kommunikationssystems X3/X5/X8 durchgeführt.</p> <p>Beschreibung siehe Integration ins Kunden-LAN.</p> <p>Für die Besonderheiten bei der Konfiguration siehe Konfiguration der UC Booster Card</p>
<p>Basiskonfiguration</p> <p>Die Basiskonfiguration wird zusammen mit der Erstinstallation des OpenScape Business Kommunikationssystems X3/X5/X8 durchgeführt.</p> <p>Beschreibung siehe Basiskonfiguration.</p>	<p>Basiskonfiguration</p> <p>Die Basiskonfiguration wird nachträglich an einem bereits konfigurierten OpenScape Business Kommunikationssystems X3/X5/X8 durchgeführt.</p> <p>Beschreibung siehe Basiskonfiguration.</p> <p>Für die Besonderheiten bei der Basiskonfiguration siehe Basiskonfiguration</p>
<p>Abschließende Tätigkeiten</p> <p>Die abschließenden Tätigkeiten (inkl. Lizenzierung der UC Clients) werden zusammen mit der Erstinstallation des OpenScape Business Kommunikationssystems X3/X5/X8 durchgeführt.</p> <p>Beschreibung siehe Abschließende Tätigkeiten.</p>	<p>Abschließende Tätigkeiten</p> <p>Die abschließenden Tätigkeiten (inkl. Lizenzierung der UC Clients) werden zusammen mit der Erstinstallation des OpenScape Business Kommunikationssystems X3/X5/X8 durchgeführt.</p> <p>Beschreibung siehe Abschließende Tätigkeiten.</p> <p>Für die Besonderheiten bei den abschließenden Tätigkeiten siehe Abschließende Tätigkeiten</p>

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 12 SP5 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
<p>Installation des Linux-Servers</p> <p>Die Installation des Linux-Servers ist in der OpenScape Business Linux-Server Installationsanleitung beschrieben.</p>	<p>Installation des Linux-Servers</p> <p>Die Installation des Linux-Servers ist in der OpenScape Business Linux-Server Installationsanleitung beschrieben.</p>
Installation der Kommunikationssoftware	Installation der Kommunikationssoftware
<p>Konfiguration des UC Booster Servers</p> <p>Die Konfiguration des UC Booster Servers wird zusammen mit der Erstinstallation des OpenScape Business Kommunikationssystems X3/X5/X8 durchgeführt.</p> <p>Beschreibung siehe Integration ins Kunden-LAN.</p>	<p>Konfiguration des UC Booster Servers</p> <p>Die Konfiguration des UC Booster Servers wird nachträglich an einem bereits konfigurierten OpenScape Business Kommunikationssystems X3/X5/X8 durchgeführt.</p> <p>Beschreibung siehe Integration ins Kunden-LAN.</p> <p>Für die Besonderheiten bei der Konfiguration siehe Konfiguration des UC Booster Servers</p>
<p>Basiskonfiguration</p> <p>Die Basiskonfiguration wird zusammen mit der Erstinstallation des OpenScape Business Kommunikationssystems X3/X5/X8 durchgeführt.</p> <p>Beschreibung siehe Basiskonfiguration.</p>	<p>Basiskonfiguration</p> <p>Die Basiskonfiguration wird nachträglich an einem bereits konfigurierten OpenScape Business Kommunikationssystems X3/X5/X8 durchgeführt.</p> <p>Beschreibung siehe Basiskonfiguration.</p> <p>Für die Besonderheiten bei der Basiskonfiguration siehe Basiskonfiguration</p>
<p>Abschließende Tätigkeiten</p> <p>Die abschließenden Tätigkeiten (inkl. Lizenzierung der UC Clients) werden zusammen mit der Erstinstallation des OpenScape Business Kommunikationssystems X3/X5/X8 durchgeführt.</p> <p>Beschreibung siehe Abschließende Tätigkeiten.</p>	<p>Abschließende Tätigkeiten</p> <p>Die abschließenden Tätigkeiten (inkl. Lizenzierung der UC Clients) werden zusammen mit der Erstinstallation des OpenScape Business Kommunikationssystems X3/X5/X8 durchgeführt.</p> <p>Beschreibung siehe Abschließende Tätigkeiten.</p> <p>Für die Besonderheiten bei den abschließenden Tätigkeiten siehe Abschließende Tätigkeiten</p>

6.1 Voraussetzungen für die Ersteinrichtung

Die Erfüllung der Voraussetzungen für die Ersteinrichtung gewährleistet den Betrieb von OpenScape Business UC Booster.

Allgemeines

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

- Das Kommunikationssystem OpenScape Business X3/X5/X8 ist konfiguriert und betriebsbereit.
- Die LAN-Infrastruktur (Internet-Router, Switches, usw.) ist vorhanden und nutzbar.
- Die IP-Telefone sind an das Kunden-LAN angeschlossen.
- Ein Breitband-Internetzugang wird für Software-Updates und Remote-Zugang empfohlen.
- Alle für OpenScape Business UC Booster benötigten Lizenzen sind vorhanden (z. B. UC Clients, 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.

- Netzwerkgeräte:

Ein IPv6-fähiges Netzwerkgerät, über das die UC Booster Card mit dem Kommunikationssystem verbunden ist, ist für einen ordnungsgemäßen Betrieb erforderlich. Dadurch erhält die UC Booster Card während der Ersteinrichtung und nach jedem Neustart des Systems automatisch eine IP-Adresse.

Wenn das Netzwerkgerät nicht IPv6-fähig ist, 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 Kommunikationssystems. Anschließend kann die gewünschte IP-Adresse für die UC Booster Card während der Ersteinrichtung und nach jedem Neustart des Systems eingegeben werden. Die Kommunikation zwischen System und UC Booster Card findet jetzt über die IPv4-Verbindung des Switches statt.

Anmerkung: 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 neueste, freigegebene Software-Version aktualisiert werden. Dabei ist zu beachten, dass das Image inkl. der UC Booster Card-Software für diesen Zweck verwendet wird.
- Webbrowser:
Für die Ersteinrichtung der UC Booster Card mit dem OpenScape Business Assistant (WBM) wird der Admin-PC verwendet. Das WBM ist browserbasiert und somit betriebssystemunabhängig. Es ist eine Bildschirmauflösung von 1024 x 768 oder höher erforderlich.
Es werden nachfolgende HTML 5 fähige Web-Browser unterstützt:
 - Microsoft Internet Explorer ab Version 10
 - Microsoft Edge
 - Mozilla Firefox ab Version 17
 - Google ChromeFalls eine ältere Webbrowser-Version installiert ist, muss eine aktuelle Version installiert werden, bevor mit der Ersteinrichtung des Systems begonnen werden kann.

Anmerkung: Uneingeschränkter Netzwerkzugriff ist zwischen OSCC und OCAB erforderlich.

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 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 dieselbe, neueste, freigegebene Software-Version aktualisiert werden.
- DVD mit Linux-Betriebssystem SLES 12 SP5 64 Bit

Ersteinrichtung OpenScape Business UC Booster

Sicherung der Konfigurationsdaten des Kommunikationssystems

Die Linux-DVD wird ggf. bei der Installation der OpenScape Business-Kommunikationssoftware benötigt, wenn Software-Pakete (RPM), die für die Kommunikationssoftware benötigt werden, nachinstalliert werden müssen.

- Webbrowser:

Für die Ersteinrichtung 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 ist eine Bildschirmauflösung von 1024 x 768 oder höher erforderlich.

Es werden nachfolgende HTML 5 fähige Web-Browser unterstützt:

- Microsoft Internet Explorer ab Version 10 (Admin-PC)
- Microsoft Edge
- Mozilla Firefox ab Version 17 (Linux-Server/Admin-PC)
- Google Chrome

Falls eine ältere Webbrowser-Version installiert ist, muss eine aktuelle Version installiert werden, bevor mit der Ersteinrichtung des Systems 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 eine 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 UC-Lösung UC Smart oder 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..._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.

Anmerkung: 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 externe 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 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 12 SP5 korrekt auf dem Linux-Server installiert und gestartet..
- DVD oder .ISO-Datei mit OpenScape Business Kommunikationssoftware.
- DVD oder .ISO-Datei mit Linux-Betriebssystem SLES 12 SP5 64 Bit für die eventuell benötigte Nachinstallation von Software-Pakete (RPM).
- Die Root-Zugangsdaten (Benutzername und Passwort) für die Anmeldung 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 OpenScapeBusiness DVD oder .ISO-Datei 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**. Sollte dies auftreten, müssen Sie zu SLES 12 DVD, für SLES 12 SP5 ISO-Datei später zurück wechseln.
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.

Anmerkung: 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):
 - **Standard-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):** IP-Adresse des DNS-Servers, während der Linux-Installation angegeben. Ist im internen Netz kein DNS-Server vorhanden, tragen Sie hier die IP-Adresse des Internet-Routers ein (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.
 - **Netzmaske:** Die während der Linux-Installation angegebene Subnetzmaske des Linux-Servers, z. B.: 255.255.255.0.
 - **Beginn des IP-Bereichs** und **Ende des IP-Bereichs:** IP-Adressbereich, aus dem der DHCP-Server IP-Adressen zuweisen kann, 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 12 DVD oder .ISO-Datei einzulegen. Legen Sie die DVD oder .ISO-Datei ein und bestätigen Sie mit **Continue**. Legen Sie nach erfolgreicher Installation der RPM-Pakete wieder die OpenScape Business DVD oder .ISO-Datei 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.

Anmerkung: Es dauert einige Minuten, bis alle Komponenten der OpenScape Business Kommunikationssoftware aktiv sind.

6.4.2 Konfiguration des UC Booster Servers

Während der Erstkonfiguration 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 der OpenScape Business UC Booster Card sind folgende Konfigurationsanteile wichtig.

- Auswahl der UC-Lösung

Es kann ausgewählt werden, ob die UC-Lösung UC Smart oder 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.

6.4.2.1 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.

Anmerkung: 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 (*).

Anmerkung: 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.

Anmerkung: 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**.

6.4.3 Software-Update für die 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..._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 Clients wird getrennt.

Beschreibung der IP-Adressänderung siehe [Systemeinstellungen](#).

3) Änderung der Applikationsauswahl

Ändern Sie im WBM des Kommunikationssystems mit dem Wizard **Erstinstallation** bei der Nutzung von UC Suite die Applikationsauswahl von **Paket mit UC Suite** auf **Paket mit UC Suite auf OSBiz UC Booster Server** oder bei der Nutzung von UC Smart die Applikationsauswahl von **Paket mit UC Smart** auf **Paket mit UC Smart 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 [Updates](#).

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 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.

Eine aktuelle und vollständige Liste aller verwendeten Ports von OpenScape Business finden Sie in der „Interface Management Database“ (IFMD), die über das Partnerportal von Unify (<https://unify.com/en/partners/partner-portal>) zugänglich ist.

Anmerkung: Die in der folgenden Liste mit „O“ gekennzeichneten Ports sind optional, d. h. sie sind in der Firewall nicht permanent geöffnet.

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

Ersteinrichtung OpenScape Business UC Booster

Beschreibung	TCP	UDP	Portnummer	OpenScape Business X	UC Booster Card	OpenScape Business S	UC Booster Server
CLS	X		7780 7790	O		O	
Communication Client-Installationsprogramm	X		8101	X	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	
HFA	X		4060	X		X	
HFA Secure	X		4061	X		X	
Instant Messaging (http)	X		8101	X	X	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
xNAT traversal (NAT-T)		X	4500	X			
NTP		X	123	X			
xOpenfire Admin (https)	X		9091		X	X	X
OpenScape Business Auto Update Service (http)	X		8101	X	X	X	X
OpenScape Business Multisite	X		8778		X	X	X

Ersteinrichtung OpenScape Business UC Booster

Beschreibung	TCP	UDP	Portnummer	OpenScape Business X	UC Booster Card	OpenScape Business S	UC Booster Server
OpenScape Business myReports (http)	X		8101		X	X	X
OpenScape Business Status Server	X		8808	X		X	X
OpenScape Business Benutzerportal	X	X	8779		X	X	X
Postgres	X		5432	X	X	X	X
RTP (eingebettet)		X	29100-30530	X	X	X	X
RTP (Server)		X	29100-30888	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	
VSL	X		8770-8780		X	X	X
Webadmin for Clients	X		8803	X	X	X	X
Webbased Clients							
Webbased Clients (http)	X		8801	X	X	X	X
Webbased Clients (https)	X		8802	X	X	X	X

Anmerkung: 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.

Anmerkung: Es empfiehlt sich, keine Lizenzdateien zu installieren oder einen Assistenten auszuführen, wenn das System aktiv ist, da dadurch aktive Anrufe möglicherweise beendet werden könnten.

Activation Period

Innerhalb der Activation Period (Zeitspanne von 30 Tagen) muss die Lizenzaktivierung vorgenommen werden. Die Activation Period beginnt, wenn im WBM das aktuelle Datum eingegeben wird. Dabei wird das Ablaufdatum der Activation Period gespeichert.

Das Produkt ist während der Activation Period voll funktionsfähig und die maximale Anzahl an Lizenzen steht zur Nutzung zur Verfügung.

Verliert das System innerhalb der Activation Period das aktuelle Datum (z. B. durch eine Entladung des Akkus auf dem Mainboard), muss zeitnah im WBM das Datum aktualisiert werden, damit das System innerhalb der Activation Period weiterhin uneingeschränkt genutzt werden kann.

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. Dies ist auch die 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.

Zugehörige Konzepte

[Teilnehmer](#) auf Seite 209

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 ID Locking](#)).

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 Netzwerk 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 Netzwerk

Für einen OpenScape Business Netzwerk wird eine netzweite Lizenzdatei (Netzwerklicenzdatei) 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 Netzwerks können die Lizenzen über das WBM verschoben werden.

Bei der Lizenzierung eines Netzwerks ist eine Online-Aktivierung nicht möglich.

Pay As You Go

Neben dem traditionellen Lizenzierungsmodell unterstützt OpenScape Business auch ein Abonnement-Lizenzierungsmodell (Pay As You Go). "Pay As You Go" bietet die Möglichkeit, nur die genutzten Lizenzen pro Abrechnungszeitraum in Rechnung zu stellen und zusätzliche Lizenzen zu nutzen, ohne die Lizenzdatei zu erweitern. Es ist nicht erforderlich, die Anzahl der Lizenzen im Voraus festzulegen.

Eine permanente Internetverbindung vom OpenScape Business-System zum Central License Server (CLS) ist erforderlich. Sie kann entweder online mit einem Lizenzaktivierungscode (LAC) oder per Datei-Upload aktiviert werden. Nach der Installation, der kundenspezifischen Konfiguration der Lösung und der Aktivierung von "Pay As You Go" wird in regelmäßigen Abständen ein Bericht über die genutzten Lizenzen an den Central License Server (CLS) gesendet und ausgewertet. Einmal im Monat wird ein Abschlussbericht auf der Produktseite des Central License Server (CLS) erstellt, und der Inhalt dieses Abschlussberichts wird für die Lizenzabrechnung verwendet.

Mit der Abonnementlizenzierung wird ein neuer Zeitraum eingeführt, die Wartezeit. Die Wartezeit beginnt mit dem Systemstart, oder wenn eine "Pay As You Go"-Lizenzdatei aktiviert wird. Nachfolgend beginnt der Zeitraum. Eine während dieses Zeitraums im WBM vorgenommene Lizenzkonfiguration führt zudem nicht zu einer Aktualisierung der Lizenznutzung. Die maximale Dauer der Wartezeit beträgt 2 Stunden.

Anmerkung: Damit die Firewall auf das CLS zugreifen kann, sind folgende Maßnahmen erforderlich:

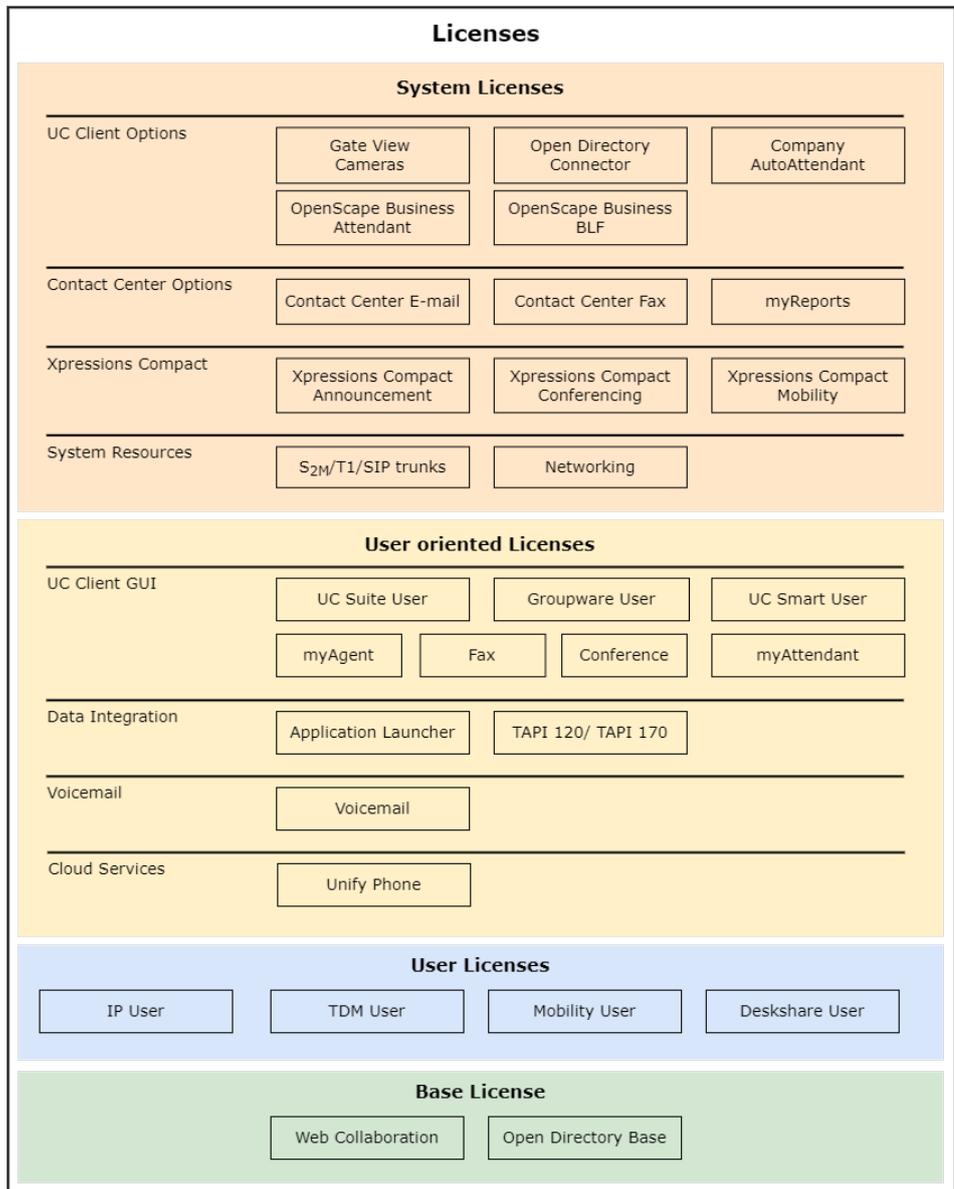
-) Die Ports 7780 und 7790 Ports wurden für ausgehenden IP-Datenverkehr freigegeben
 -) 188.64.16.4 wurde für ausgehenden IP-Datenverkehr freigegeben.
-

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.

Zugehörige Konzepte

Voraussetzungen für myPortal Smart

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 stehen zur Verfügung:

- **OpenScape Business V2 X1 Base**

Für die Freischaltung des V2-Funktionsumfangs von

- OpenScape Business X1

Die Basislizenz enthält zusätzlich die Lizenzen OpenDirectory Base für die Nutzung von Open Directory Service (ODS) und Web Collaboration für das Starten einer Web Collaboration Sitzung. Damit kann die UC-Lösung UC Smart mit einer externen Datenbank verbunden werden.

- **OpenScape Business V2 Base**

Für die Freischaltung des V2-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) und Web Collaboration für das Starten einer Web Collaboration Sitzung. Damit können die UC-Lösungen UC Suite oder UC Smart mit einer externen Datenbank verbunden werden.

7.2.2 Benutzerlizenzen

Jeder am Kommunikationssystem angeschlossene Teilnehmer benötigt für die externe Telefonie eine Benutzerlizenz. Diese Lizenz wird der Rufnummer des Teilnehmers über das WBM fest zugeordnet.

Benutzerlizenzen beinhalten die umfassende Sprachfunktionalität 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-Teilnehmer**

Für die Nutzung von IP-Systemtelefonen (HFA) und SIP-Telefonen.

- **TDM-Benutzer**

Für die Nutzung von UP0-Systemtelefonen, analogen Telefonen, analogem FAX, ISDN-Telefonen, ISDN-Fax und DECT-Telefonen.

- **Mobility-Teilnehmer**

Für die Nutzung von GSM-/Mobiltelefonen, Smartphones und Tablet-PCs als Nebenstelle des Kommunikationssystems. Für die Nutzung von myPortal to go und Mobility Entry. Die Zuordnung eines zusätzlichen Tischtelefons (Desk Phone) ist nicht erforderlich. Für die Verwendung des Unify Phone Clients zusammen mit OpenScape Business.

- **DeskShare User**

Für die Nutzung des Leistungsmerkmals DeskSharing. Diesen Teilnehmern ist nur eine Rufnummer und kein physikalisches Telefon fest zugeordnet. DeskShare User können bestimmte IP-Systemtelefone unter ihrer eigenen, fest zugeordneten Rufnummer nutzen und haben an den Telefonen Zugriff auf ihre persönlichen Telefoneinstellungen.

- **Fallback-Benutzer**

Für die grundlegende Telefonie im Falle des Ausfalls eines Systemknotens. Die Lizenz wird als zeitbasierte Pay As You Go-Lizenz unterstützt. Daher wird die Nutzungszeit basierend auf den Tagen berechnet, an denen das System Benutzer von anderen Knoten hostet. Die Lizenzen sind nur während dieser Host-Zeit gültig. Bei normalem Betriebsmodus werden Fallback User wie nicht lizenzierte Benutzer behandelt.

Flexible Teilnehmer-Lizenzierung

Mit der flexiblen Teilnehmer-Lizenzierung können TDM-, Mobility- und DeskShare User auch mit IP-Benutzerlizenzen lizenziert werden. Sind alle erworbenen TDM-, DeskShare- und Mobility-Benutzerlizenzen den Teilnehmern zugeordnet und besteht Bedarf für weitere TDM-, DeskShare- und Mobility-Teilnehmer, können übrige IP-Benutzerlizenzen 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 OpenScape Business eingespielt und aktiviert werden muss.

Flexible Teilnehmer-Lizenzierung für UC Suite

Mit der flexiblen Teilnehmer-Lizenzierung für UC Suite können myPortal for Desktop-Teilnehmer auch mit myPortal for Outlook-Benutzerlizenzen lizenziert werden. Sind alle erworbenen myPortal for Desktop-Lizenzen den Teilnehmern zugeordnet und besteht Bedarf für weitere Benutzer, können übrige myPortal for Outlook-Benutzerlizenzen verwendet werden, um diesen Bedarf zu decken.

Voraussetzung für die Nutzung der flexiblen Teilnehmer-Lizenzierung ist die Software-Version V2 und eine am CLS neu generierte Lizenzdatei, die in OpenScape Business eingespielt und aktiviert werden muss.

Zugehörige Konzepte

[Lizenzzuordnung \(Standalone\)](#) auf Seite 168

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.

Anmerkung: Wird die UC-Lösung UC Smart auf UC Suite erweitert, bleiben die vorhandenen VoiceMail-Lizenzen und die Zuordnung zu den Teilnehmern erhalten.

Cloud-Dienste

- **Unify Phone**

Für die Verwendung des Unify Phone Clients zusammen mit OpenScape Business.

UC Client Benutzeroberfläche

- **UC Smart User**

Für die Nutzung der UC Smart Funktionen der Communications Clients myPortal @Work, myPortal to go und weiterer Web Services-Clients.

- **UC Suite User**

Für die Nutzung der UC Suite Funktionen der Communications Clients myPortal @work, myPortal for Desktop, myPortal to go und weiterer Web Services-Clients.

- **Groupware User**

Für die Nutzung der UC Suite Funktionen der Communications Clients myPortal @work, myPortal for Outlook, myPortal to go und weiterer Web Services-Clients.

- **Faxnr.**

Für die Nutzung einer Faxbox innerhalb der UC Suite. Voraussetzung ist eine zusätzliche UC User- oder eine Groupware User-Lizenz.

- **Konferenz**

Für die Nutzung der Konferenz-Verwaltung innerhalb der UC Suite, wie z.B. Verwalten und Einleiten von permanenten und wiederkehrenden Konferenzen. Voraussetzung ist eine zusätzliche UC 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 und Zugriff auf die Anruflhistorie.

Anmerkung: Für den mobilen Client myPortal to go ist neben der Mobility User-Lizenz eine zusätzliche UC User-Lizenz oder Groupware User-Lizenz für die UC-Lösung UC Smart oder die UC-Lösung UC Suite erforderlich.

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, UC Suite oder myAgent betrieben werden und benötigt zusätzlich eine UC User-/Groupware User-Lizenz oder eine myAgent-Lizenz. Optional kann er den Open Directory Service nutzen.
- **OpenScape Business TAPI**
Für die Nutzung von TAPI-konformen Applikationen und zum PC-unterstützten 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.

Übersicht über Systemlizenzanforderungen

Trunktype	SSP-Lizenz	Leitungslizenz Kanal	Networking-Lizenz
ITSP	Ja	Ja	Nein
Native SIP-Trunk	Ja	Nein	Ja
Skype for Business	Ja	Ja	Nein
Circuit	Ja	Nein	Nein
Unify Phone	Ja	Nein	Nein
SIPQ-Verbindung	Nein	Nein	Ja

Folgende Systemlizenzen stehen zur Verfügung.

System Ressourcen

- **S_{2M}/T1/SIP Trunks**

Für die Nutzung von S_{2M}-/T1- und ITSP-Kanälen. S₀-Kanäle müssen nicht lizenziert werden. Dazu zählen auch Anschaltungen zu S₀-Fax-Servern im PP-Modus. Bei Primärmultiplex-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.

- **Vernetzung**

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 ist eine Lizenz nötig.

Anmerkung: 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 3: Übersicht über die Systemressourcenlizenzen (S_{2M}/ITSP)

Protokoll	Lizenzen			
	Keine Lizenz	OpenScape Business Networking (1x pro System)	OpenScape Business S _{2M} / ITSP (1x pro Kanal)	TDM-Teilnehmer
S₀ intern				
Fax-Server (DSS1/QSIG)	X			
Euro-Bus				Pro S ₀ -Teilnehmer
S₀ - Amtsleitungen				
Euro-Amt PP	X			
Euro-Amt PMP	X			
S_{2M} - Amtsleitungen				
Euro-Amt PP			X	
ITSP - Provider				
ITSP 1 bis 8			X	
S₀ Vernetzung				
QSIG		X		

Protokoll	Lizenzen			
	Keine Lizenz	OpenScape Business Networking (1x pro System)	OpenScape Business S _{2M} / ITSP (1x pro Kanal)	TDM-Teilnehmer
CorNet-NQ		X		
S_{2M} - 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 sechs 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 sechs 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 Berichtsvorlagen erfolgt über den Report Manager mit der Möglichkeit zur Umgruppierung sowie zum Hinzufügen und Löschen neu erstellter Report-Vorlagen.

UC Client Optionen

- **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.

- **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 oder UC User-Lizenz nötig.

- **OpenScape Business BLF**

Für die Nutzung der zusätzlichen Besetztlampenfeldanzeige von OpenScape Business BLF. Pro Teilnehmer ist eine BLF-Lizenz und eine UC User-Lizenz erforderlich. Pro Knoten können bis zu 50 OpenScape Business BLF lizenziert werden.

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 V3 Service Evaluierung**

Diese Evaluierungslizenz ist für Partner bestimmt, die das Kommunikationssystem in ihrer Firma vorkonfigurieren und später beim Kunden in Betrieb nehmen möchten. Während der Vorkonfiguration startet die Activation Period von 30 Tagen. Damit nach Inbetriebnahme des Systems die Activation Period von 30 Tagen neu startet, muss diese Evaluierungslizenz nach der Inbetriebnahme beim Kunden aktiviert werden.❖

Die Aktivierung ist einmal pro System und nur innerhalb der Activation Period möglich. Ist die Activation Period abgelaufen muss das System mit dauerhaften Lizenzen lizenziert werden.

Anmerkung: Wenn die Service-Evaluierung aktiviert ist, kann CLS Connect nicht aktiviert werden.

- **OpenScape Business V3 UC Smart Evaluierung**

Diese Evaluierungslizenz ist für Kunden bestimmt, die die UC-Funktionen von UC Smart testen möchten. Mit dieser Evaluierungslizenz können alle Leistungsmerkmale von UC Smart genutzt werden.

Anmerkung: 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 V3 UC Suite Evaluierung**

Diese Evaluierungslizenz ist für Kunden bestimmt, die die UC-Funktionen von UC Suite testen möchten. Mit dieser Evaluierungslizenz können alle Leistungsmerkmale von UC Suite genutzt werden.

Anmerkung: 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 V3 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.

Anmerkung: 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.). Andernfalls können in OpenScape Business Fehler auftreten.

- **OpenScape Business V3 CRM Evaluierung**

Diese Evaluierungslizenz ist für Kunden bestimmt, Application Launcher, Open Directory Service und TAPI testen möchten.

- **OpenScape Business V3 Attendant Evaluierung**

Diese Evaluierungslizenz ist für Kunden bestimmt, die die Applikation OpenScape Business Attendant testen möchten.

- **OpenScape Business V3 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 Upgrade-Lizenzen

Upgrade-Lizenzen sind nötig, um von HiPath 3000 V9, OpenScape Office V3 und OpenScape Business V1 Systemen auf OpenScape Business V2 Systeme 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 Upgrade-Lizenz auf OpenScape Business hochgerüstet werden.

Folgende Upgrade-Lizenzen stehen zur Verfügung:

- **HiPath 3000 V9 Upgrade auf OpenScape Business V2**

Für die Migration von HiPath 3000 V9 auf OpenScape Business V2 X3/X5/X8.

- **HiPath 3000 V8 Upgrade auf OpenScape Business V2**

Für die Migration von HiPath 3000 V8 auf HiPath 3000 V9 und anschließend auf OpenScape Business V2 X3/X5/X8.

- **HiPath 3000 V7 Upgrade auf OpenScape Business V2**

Für die Migration von HiPath 3000 V7 auf HiPath 3000 V9 und anschließend auf OpenScape Business V2 X3/X5/X8.

- **OpenScape Office V3 MX/LX Upgrade auf OpenScape Business V2**

Für die Migration von OpenScape Office V3 MX/LX auf OpenScape Business V2.

7.2.7 Vorschläge für Lizenzkombinationen

Lizenzen können beliebig kombiniert werden. Im Folgenden sind einige Vorschläge aufgelistet, wie Lizenzen sinnvoll kombiniert werden können, um die gewünschten Funktionen zu nutzen.

Bitte beachten Sie, dass für manche Funktionen mehrere Lizenzen benötigt werden.

Telefonie

- Erforderlich: Teilnehmer-Lizenz IP User oder TDM-Teilnehmer oder DeskShare User

Anmerkung: Ohne gültige Lizenz ist das Telefon nur für interne Verbindungen freigeschaltet.

Tefonie mit UC Smart

- Telefonie mit Sprachbox (UC Smart)
 - Erforderlich: Teilnehmer-Lizenz IP User oder TDM-Teilnehmer oder DeskShare User
 - Erforderlich: User-orientierte VoiceMail-Lizenz
- Telefonie mit Mobility Entry (DISA-basiertes Mobility)
 - Erforderlich: Teilnehmer-Lizenz Mobility-Teilnehmer
- Telefonie mit myPortal to go
 - Erforderlich: Teilnehmer-Lizenz Mobility-Teilnehmer
 - In der Betriebsart **Desktelefon** (Steuerung des Bürotelefons) ist keine Lizenz Mobility-Teilnehmer erforderlich.
 - Erforderlich: User-orientierte Lizenz UC User
 - Optional: User-orientierte VoiceMail-Lizenz
- Telefonie mit myPortal @work
 - Erforderlich: IP-Teilnehmer
 - Erforderlich: User-orientierte Lizenz UC User
 - Optional: User-orientierte VoiceMail-Lizenz
 - Optional: User-orientierte Lizenz Konferenz
- Telefonie mit myPortal @work VoIP
 - Erforderlich: IP-Teilnehmer
 - Erforderlich: User-orientierte Lizenz UC User
 - Optional: User-orientierte VoiceMail-Lizenz
 - Optional: User-orientierte Lizenz Konferenz
- Telefonie mit optiClient Attendant
 - Erforderlich: Teilnehmer-Lizenz IP User oder TDM-Teilnehmer oder DeskShare User
 - Erforderlich: Systemlizenz OpenScape Business Attendant
 - Optional: User-orientierte VoiceMail-Lizenz
 - Optional: User-orientierte Lizenz UC User (zum Anzeigen des Anwesenheitsstatus)

Telefonie mit UC Suite

- Telefonie mit Sprachbox (UC Suite)
 - Erforderlich: Teilnehmer-Lizenz IP User oder TDM-Teilnehmer oder DeskShare User
 - Erforderlich: User-orientierte VoiceMail-Lizenz
- Telefonie mit myPortal for Desktop
 - Erforderlich: Teilnehmer-Lizenz IP User oder TDM-Teilnehmer oder DeskShare User
 - Erforderlich: User-orientierte Lizenz UC User
 - Optional: User-orientierte VoiceMail-Lizenz
 - Optional: User-orientierte Lizenz Fax
 - Optional: User-orientierte Lizenz Konferenz
- Telefonie mit myPortal for Outlook
 - Erforderlich: Teilnehmer-Lizenz IP User oder TDM-Teilnehmer oder DeskShare User
 - Erforderlich: User-orientierte Lizenz Groupware User
 - Optional: User-orientierte VoiceMail-Lizenz
 - Optional: User-orientierte Lizenz Fax
 - Optional: User-orientierte Lizenz Konferenz
- Telefonie mit myPortal to go
 - Erforderlich: Teilnehmer-Lizenz Mobility-Teilnehmer
In der Betriebsart **Desktelefon** (Steuerung des Bürotelefons) ist keine Lizenz Mobility-Teilnehmer erforderlich.
 - Erforderlich: User-orientierte Lizenz Groupware User oder UC User
 - Optional: User-orientierte VoiceMail-Lizenz
- Telefonie mit myPortal @work
 - Erforderlich: IP-Teilnehmer
 - Erforderlich: User-orientierte Lizenz Groupware User oder UC User
 - Optional: User-orientierte VoiceMail-Lizenz
 - Optional: User-orientierte Lizenz Konferenz
- Telefonie mit myPortal @work VoIP
 - Erforderlich: IP-Teilnehmer
 - Erforderlich: User-orientierte Lizenz Groupware User oder UC User
 - Optional: User-orientierte VoiceMail-Lizenz
 - Optional: User-orientierte Lizenz Konferenz
- Telefonie mit myAttendant
 - Erforderlich: Teilnehmer-Lizenz IP User oder TDM-Teilnehmer oder DeskShare User
 - Erforderlich: User-orientierte Lizenz myAttendant
 - Optional: User-orientierte VoiceMail-Lizenz

Lizenzierung

Lizenzierung eines Kommunikationssystems (Standalone)

Telefonie mit Unify Phone

- Erforderlich: IP-Teilnehmer
- Erforderlich: User-orientierte Unify Phone-Lizenz
- Optional: User-orientierte VoiceMail-Lizenz und zusätzliche IP-User-Lizenz für die Teamkonfiguration

Nutzung des Contact Centers

- Erforderlich: Teilnehmer-Lizenz IP-Teilnehmer, DeskShare User oder Mobility-Teilnehmer
- Erforderlich: User-orientierte Lizenz myAgent

Damit das System Contact Center-Anrufe weiterleiten und adressieren kann, muss mindestens eine myAgent-Lizenz aktiv sein.

- Optional: Systemlizenz Contact Center E-Mail
- Optional: Systemlizenz Contact Center Fax
- Optional: Systemlizenz myReports

Nutzung des Company AutoAttendant

- Erforderlich: Systemlizenz Company AutoAttendant

Die AutoAttendant-Systemlizenz des Unternehmens muss aktiv sein, damit das System AutoAttendant-Anrufe weiterleiten und adressieren kann.

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.

Zugehörige Konzepte

[Lizenzaktivierung \(Standalone\)](#) auf Seite 167

[Lizenzzuordnung \(Standalone\)](#) auf Seite 168

7.3.1 CLS Connect

CLS Connect ermöglicht Ihnen unbegrenzte Rehosts Ihrer OpenScape Business-Systeme. Zu diesem Zweck muss das **CLS Connect**-Flag aktiviert werden.

Anmerkung: Nach der Aktivierung kann dieses Flag nicht mehr ausgeschaltet werden.

Wenn das System die Verbindung zum CLS verliert, beginnt der Failover-Zeitraum. Wenn die Verbindung nach 30 Tagen nicht wiederhergestellt ist, wird das System in den Notfallmodus versetzt und gilt als unlizenziert.

Anmerkung: Wenn ein OpenScape Business-System mit aktivem CLS Connect neu programmiert werden muss, kann keine Sicherungsdatei erstellt werden. Ein Reload muss mit der gleichen MAC-ID und SIEL-ID durchgeführt werden. CLS Connect lässt sich ohne aktive Basislizenz nicht aktivieren. Die vorhandene Lizenzdatei aus dem CLS kann manuell über das WBM in das System hochgeladen werden.

7.3.2 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 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** und kann falls nötig vom Administrator mit Profil **Expert** geändert werden.

Anmerkung: Für die Online-Lizenzaktivierung wird standardmäßig der Port 7790 verwendet. Dieser Port muss in der Firewall des Kundennetzes freigegeben sein.

Anmerkung: 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** 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.

Anmerkung: Zusätzlich erworbene Lizenzen können auch über Remote aktiviert werden.

Zugehörige Konzepte

[Lizenzierung eines Kommunikationssystems \(Standalone\)](#) auf Seite 166

[Lizenzzuordnung \(Standalone\)](#) auf Seite 168

7.3.3 Lizenzzuordnung (Standalone)

Nach erfolgreicher Aktivierung müssen die erworbenen Lizenzen den Teilnehmern und Leitungen zugeordnet werden. Systemweite Leistungsmerkmale sind in einem Standalone-System bereits mit der Aktivierung freigeschaltet.

Zuordnung von Benutzerlizenzen und User-orientierten Lizenzen

Den Teilnehmern können Benutzerlizenzen und User-orientierte Lizenzen zugeordnet werden.

Folgenden Anwender-Typen können Benutzerlizenzen zugeordnet werden:

Symbol	Benutzerlizenz	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
	Mobility-Teilnehmer	Für die Nutzung von myPortal to go, Mobility Entry und DISA (One Number Service)
	Deskshare User	Für die Nutzung von DeskSharing für IP-Teilnehmer

Die Benutzerlizenzen werden den Rufnummern der Teilnehmer fest zugeordnet. Wird ein Teilnehmer gelöscht oder einer Rufnummer ein anderer Teilnehmer-Typ zugeordnet, wird die zugehörige Benutzerlizenz freigegeben.

Neben einigen Lizenzen befindet sich ein Sternchen. Ein rotes Sternchen bedeutet, dass die Lizenzen auch durch die Zuweisung einer anderen Lizenz gedeckt werden können.

Mit der flexiblen Lizenzierung können TDM-, Mobility- und DeskShare-Teilnehmer auch mit IP-Benutzerlizenzen lizenziert werden. Sind alle erworbenen TDM-, DeskShare- und Mobility-Benutzerlizenzen den Teilnehmern zugeordnet und besteht Bedarf für weitere TDM-, DeskShare- und Mobility-Teilnehmer, können übrige IP-Benutzerlizenzen verwendet werden, um diesen Bedarf zu decken.

Nachdem dem Teilnehmer eine Benutzerlizenz zugeordnet wurde, können diesem Teilnehmer auch User-orientierte Lizenzen zugeordnet werden.

Folgende User-orientierte Lizenzen können den Teilnehmern zugeordnet werden:

Symbol	User-orientierte Lizenz	Beschreibung
	Voicemail	Für die Nutzung der Sprachbox.
	Groupware User	Für die Nutzung der UC Suite-Funktionen über myPortal for Outlook.

Symbol	User-orientierte Lizenz	Beschreibung
	RAS-Benutzer	Für die Nutzung der UC Suite-Funktionen über myPortal for Desktop.
	Fax	Für die Nutzung einer Faxbox innerhalb der UC Suite. Voraussetzung ist eine UC User- oder eine Groupware User-Lizenz.
	Konferenz	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.
	Unify Phone	Für die Nutzung des Unify Phone-Clients in Kombination mit OpenScope Business.
	TAPI	Für die Nutzung von TAPI-konformen Applikationen und zum PC-unterstützten Telefonieren mit kundeneigenen Programmen verschiedener Software-Hersteller.

Sie können sich eine Übersicht über alle Benutzerlizenzen und User-orientierte Lizenzen anzeigen lassen (über **Lokale Benutzerlizenzen > Übersicht**).

In dieser Übersicht werden Ihnen auch zu jedem Teilnehmer die Zustände seiner Lizenzen angezeigt.

Es gibt folgende Lizenzzustände:

Successfully licensed
 Not licensed
 License demand configurable
 License demand not configurable
 Unsaved license release
 Unsaved license demand release
 Unsaved license demand

Zuordnung von System-Lizenzen

System-Lizenzen enthalten Lizenzen für Leitungen und systemweite Leistungsmerkmale.

Folgenden Typen von Leitungen können Lizenzen zugeordnet werden:

- S_{2M}-/T1-Leitungen: Anzahl der B-Channels

- ITSP-Leitungen: Anzahl der gleichzeitig über einen ITSP geführten Rufe

Lizenzen für systemweite Leistungsmerkmale werden bei einem Standalone-System bereits bei der Lizenzaktivierung standardmäßig freigeschaltet. Eine weitere Zuordnung ist nicht erforderlich.

Vorgehensweise bei der Lizenzzuordnung

Voraussetzung: Die Lizenzdatei ist aktiviert und die Teilnehmer sind eingerichtet.

- Teilnehmer lizenzieren
 - 1)** Teilnehmer eine User-Lizenz zuordnen. Durch diese Zuordnung wird für den Teilnehmer eine Lizenzanforderung generiert und zugleich die Zuordnung der User-orientierten Lizenzen freigeschaltet.
 - 2)** 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](#)).
 - 3)** Lizenzanforderungen prüfen und freischalten.
 - 4)** 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.

Anmerkung: Zur besseren Übersicht können Sie sich die Lizenzzuordnungen für alle Teilnehmer als Vorab-Ausdruck anzeigen lassen (über **Lokale Benutzerlizenzen > Übersicht > Drucken**). Am Ende des Ausdrucks werden alle ungültigen Zuordnungen in einer separaten Tabelle aufgeführt.

- Leitungslizenzen zuordnen

Die Leitungslizenzen müssen auf die benötigten S_{2M}-/T1- und ITSP-Leitungen aufgeteilt werden.

Zugehörige Konzepte

[Lizenzierung eines Kommunikationssystems \(Standalone\)](#) auf Seite 166

[Lizenzaktivierung \(Standalone\)](#) auf Seite 167

[Benutzerlizenzen](#) auf Seite 155

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 Netzwerkverbund zusammengeschlossen, erfolgt die Lizenzierung zentral über eine Netzwerklizenzdatei, die am Master-Knoten aktiviert wird. Zusätzlich benötigt jeder Slave-Knoten im Netzwerkverbund 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 Netzwerkverbund als Master-Knoten und Slave-Knoten konfiguriert. Der Master-Knoten enthält den zentralen Lizenzagenten (zentraler CLA, central Customer License Agent). Alle Slave-Knoten im Netzwerkverbund 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 Netzwerkverbund 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 Netzwerkverbunds. 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 Netzwerkverbund 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 Netzwerkverbund neu lizenziert werden.

Lizenzierungsablauf im Netzwerkverbund anhand des o.g. Beispiels

OpenScape Business S (Master) und beide OpenScape Business X3 (Slave) sind bereits installiert, konfiguriert und zu einem Netzwerkverbund 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.

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.

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:

- **Wie Sie Lizenzdateien zu einer Netzwerklizenzdatei zusammenführen**

Sind bereits ein oder mehrere Knoten lizenziert und sollen diese in einem Netzwerk 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.

7.4.2 Lizenzzuordnung (Netzverbund)

Nach erfolgreicher Aktivierung müssen die erworbenen Lizenzen den Teilnehmern und Leitungen zugeordnet werden. Diese Zuordnung wird an jedem Knoten separat durchgeführt.

Zuordnung von Benutzerlizenzen und User-orientierten Lizenzen

Den Teilnehmern können Benutzerlizenzen und User-orientierte Lizenzen zugeordnet werden.

Folgenden Anwender-Typen können Benutzerlizenzen zugeordnet werden:

Symbol	Benutzerlizenz	Beschreibung
	IP-Teilnehmer	Für die Nutzung von IP-Systemtelefonen (HFA oder SIP) und SIP-Telefonen

Symbol	Benutzerlizenz	Beschreibung
	TDM-Teilnehmer	Für die Nutzung von UP0-Systemtelefonen, ISDN-Telefonen, analogen Telefonen und DECT-Telefonen
	Mobile Teilnehmer	Für die Nutzung von myPortal to go, Mobility Entry und DISA (One Number Service)
	DeskSharing-Teilnehmer	Für die Nutzung von DeskSharing für IP-Teilnehmer
	Fallback User	Für die grundlegende Telefonie im Falle eines Fehlerereignisses.

Die Benutzerlizenzen werden den Rufnummern der Teilnehmer fest zugeordnet. Wird ein Teilnehmer gelöscht oder einer Rufnummer ein anderer Teilnehmer-Typ zugeordnet, wird die zugehörige Benutzerlizenz freigegeben.

Mit der flexiblen Lizenzierung können TDM-, Mobility- und DeskShare-Teilnehmer auch mit IP-Benutzerlizenzen lizenziert werden. Sind alle erworbenen TDM-, DeskShare- und Mobility-Benutzerlizenzen den Teilnehmern zugeordnet und besteht Bedarf für weitere TDM-, DeskShare- und Mobility-Teilnehmer, können übrige IP-Benutzerlizenzen verwendet werden, um diesen Bedarf zu decken.

Nachdem dem Teilnehmer eine Benutzerlizenz zugeordnet wurde, können diesem Teilnehmer auch User-orientierte Lizenzen zugeordnet werden.

Folgende User-orientierte Lizenzen können den Teilnehmern zugeordnet werden:

Symbol	User-orientierte Lizenz	Beschreibung
	Voicemail	Für die Nutzung der Sprachbox.
	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 ist eine UC User- oder eine Groupware User-Lizenz.
	Konferenz	Für die Nutzung der Konferenz-Funktionen der UC Suite. Voraussetzung ist eine UC User- oder eine Groupware User-Lizenz.

Symbol	User-orientierte Lizenz	Beschreibung
	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.
	Unify Phone	Für die Nutzung des Unify Phone-Clients in Kombination mit OpenScape Business.
	TAPI 120/170	Für die Nutzung von TAPI-konformen Applikationen und zum PC-unterstützten Telefonieren mit kundeneigenen Programmen verschiedener Software-Hersteller.

Sie können sich eine Übersicht über alle Benutzerlizenzen und User-orientierte Lizenzen anzeigen lassen (über **Lokale Benutzerlizenzen > Übersicht**).

In dieser Übersicht werden Ihnen auch zu jedem Teilnehmer die Zustände seiner Lizenzen angezeigt.

Es gibt folgende Lizenzzustände:

Successfully licensed
 Not licensed
 License demand configurable
 License demand not configurable
 Unsaved license release
 Unsaved license demand release
 Unsaved license demand

Zuordnung von System-Lizenzen

System-Lizenzen enthalten Lizenzen für Leitungen und systemweite Leistungsmerkmale.

Folgenden Typen von Leitungen können Lizenzen zugeordnet werden:

- S_{2M}-/T1-Leitungen: Anzahl der B-Channels
- ITSP-Leitungen: Anzahl der gleichzeitig über einen ITSP geführten Rufe

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

- 1) Teilnehmer eine User-Lizenz zuordnen. Durch diese Zuordnung wird für den Teilnehmer eine Lizenzanforderung generiert und zugleich die Zuordnung der User-orientierten Lizenzen freigeschaltet.
- 2) 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](#)).
- 3) Lizenzanforderungen prüfen und freischalten.
- 4) 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.

Anmerkung: Zur besseren Übersicht können Sie sich die Lizenzzuordnungen für alle Teilnehmer als Vorab-Ausdruck anzeigen lassen (über **Lokale Benutzerlizenzen > Übersicht > Drucken**). Am Ende des Ausdrucks werden alle ungültigen Zuordnungen in einer separaten Tabelle aufgeführt.

- Leitungslizenzen zuordnen

Die Leitungslizenzen müssen auf die benötigten S_{2M}-/T1- und ITSP-Leitungen aufgeteilt werden.

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.

Anmerkung: 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 **InventoryInventory** auf Seite 717 abgefragt werden.

- **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 Netzwerk 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 Netzwerk (Standalone)

Es können alle dem Kommunikationssystem zugeordneten Lizenzen und die Informationen dazu angezeigt werden.

7.5.2 Lizenzinformationen im Netzwerk

In einem Netzwerk können alle Lizenzen und die Informationen dazu angezeigt werden. Diese Informationen werden aus der Netzwerklicenzdatei ausgelesen.

Die Lizenzen in einem Netzwerk 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 Netzwerk können sowohl alle Lizenzen des Netzwerkes 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.

7.6 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
- Mobile Teilnehmer

Innerhalb eines Lizenzprofils können Sie dem Teilnehmer-Typ nach Ihren Wünschen User-orientierte Lizenzen zuordnen.

Wird die Lizenzzuordnung eines Teilnehmers eines Lizenzprofils separat geändert, wird die Zuordnung des Teilnehmers zum Lizenzprofil automatisch aufgehoben.

7.7 Rehost nach Hardwaretausch

Lizenzen müssen aktualisiert werden, wenn das Mainboard der Hardwareplattform oder die Netzwerkkarte des Linux-Servers im Kommunikationssystem ausgetauscht wird. 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.

Anmerkung: Jeder Rehost wird im CLS protokolliert. Eine Lizenz kann maximal dreimal für einen Rehost verwendet werden.

Anmerkung: Die IP-Adresse des CLS kann über das WBM unter **Lizenzverwaltung > Einstellungen** abgefragt und falls nötig geändert werden.

7.8 Lizenzserver (Central License Server, CLS)

Der Lizenzserver (CLS) erzeugt und verwaltet die Lizenzdateien.

Lizenzierung

Lizenzagent (Customer License Agent, CLA)

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.

7.9 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 Netzwerkverbund, sollte nur ein CLA (zentraler CLA) auf dem Master-Knoten verwendet werden.

Folgende Konfigurationen sind möglich:

- **Wie Sie eine Verbindung zum lokalen Lizenzagenten konfigurieren**

Wird ein Knoten aus dem Netzwerkverbund 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.

- **Wie Sie die Verbindung zum zentralen Lizenzagenten ändern**

Jeder Knoten im Netzwerkverbund 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.

7.10 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 in den nicht lizenzierten Zustand zurück 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.

Wenn das System eine Änderung in ALI feststellt, wird auf der WBM-Startseite im Lizenzbereich eine Meldung angezeigt, die den Benutzer darüber informiert, dass ALI geändert wurde. Der Benutzer muss auf „Bestätigen“ klicken, um zu bestätigen, dass er über die Änderung informiert wurde. Dann wird die Nachricht von der WBM-Startseite entfernt, bis eine neue Instanz einer ALI-Änderung erkannt wird. Wenn der Benutzer nicht auf „Bestätigen“ klickt, wird die Nachricht dauerhaft auf der Startseite angezeigt.

Wichtig: Wenn Änderungen an den Parametern der Locking-ID vorgenommen werden (IP-Adresse, Gateway-Adresse, DNS-Adresse, Hostname für S-Systeme, MAC-Adresse für X-Systeme), wird die Systemlizenz ungültig. Sie sollten sich an einen autorisierten Partner am Cental License Server wenden, um eine neue Lizenzdatei zu erstellen, und die neue Lizenzdatei muss im System installiert sein.

Wichtig: Wenn ein Benutzer auf die Bestätigungsschaltfläche klickt, wird anschließend keine E-Mail gesendet. Eine E-Mail wird nur gesendet, wenn der Benutzer die Änderungen nicht über die Startseite bestätigt hat. Der E-Mail-Mechanismus wird jeden Tag mit einem 24-Stunden-Intervall ausgelöst, beginnend mit dem letzten Neustart des Systems.

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

Integration ins interne Datennetz (LAN)

DHCP

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](#)).

8.1.2 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.

8.2 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.

8.2.2 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, herstellereigene Parameter zu versorgen. Folgende

Integration ins interne Datennetz (LAN)

DNS - Namensauflösung

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

Anmerkung: Weitere Informationen zum DHCP-Server in einer Windows-Umgebung finden Sie hier: http://wiki.unify.com/wiki/DHCP_Server_in_a_Windows_environment.

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.

Weitere Informationen finden Sie im folgenden Unify Experts Wiki unter: <http://wiki.unify.com/wiki/DHCP>

DHCP-Adress-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 sich unter **Netzwerk-Schnittstellen** für den internen DHCP-Server sogar mehrere IP-Adressbereiche einrichten.

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 –

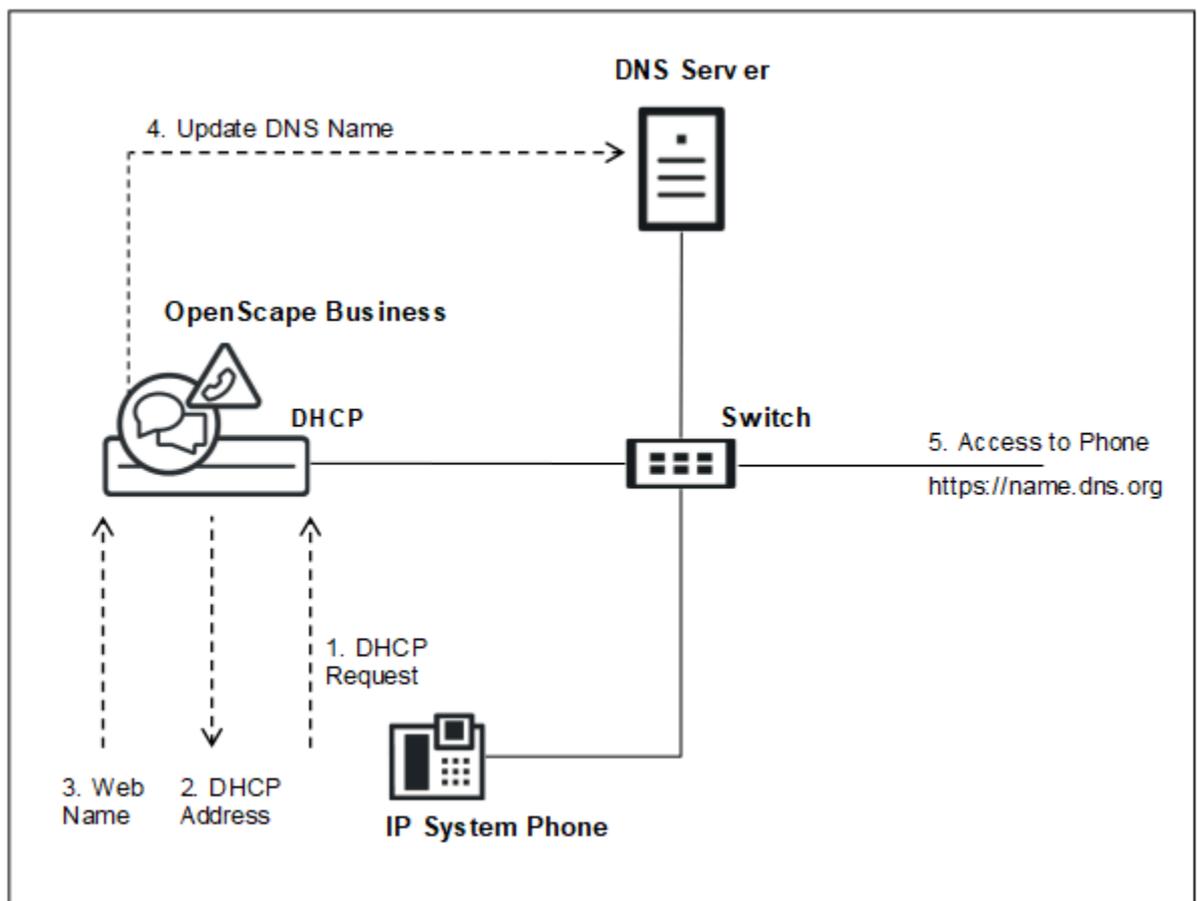
werden in der Regel eigene DNS-Server betrieben, die vom Internet unabhängig sind.

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.

Integration ins interne Datennetz (LAN)

IP-Routing

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.

8.4 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.

8.5 Deployment Service (DLI und DLS)

Mithilfe von DLI und DLS können IP-Komponenten zentral administriert und mit Software versorgt werden. Die 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. Wenn DLI für DeskPhone CP 400/600/600E/700/700X/710 aktiviert ist, werden die folgenden UC-Server-Parameter automatisch konfiguriert: UC-Protokoll, UC-Server-Adresse, UC-Server-Port.

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 integriert 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.

Anmerkung: 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

Beim 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).

Integration ins interne Datennetz (LAN)

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-and-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	Die Verwendung von SPE in Netzwerken ist möglich. DLS muss verwendet werden (DLI nicht zulässig).	Ja Die bereitzustellenden Schlüssel und Zertifikate müssen auf dem DLS verfügbar sein.
Zentrale Versorgung mehrerer unterschiedlicher Plattformen	Nein	Ja

Funktion	DLI	DLS
Freischaltung der 2. LAN-Schnittstelle der IP-Systemtelefone (PC Ethernet Mode). Siehe Grundeinstellungen > Telefonparameter-Bereitstellung	Ja	Ja

Deployment- und Licensing-Client (DLSC) (Menü)

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.

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 Internetzugang

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.

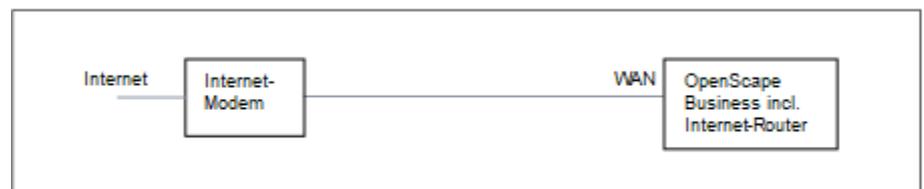
Um Internet-Telefonie nutzen zu können, benötigen Sie zusätzlich einen Internet-Telefonie-Service-Provider (ITSP, SIP-Provider).

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.

Anbindung an Service-Provider

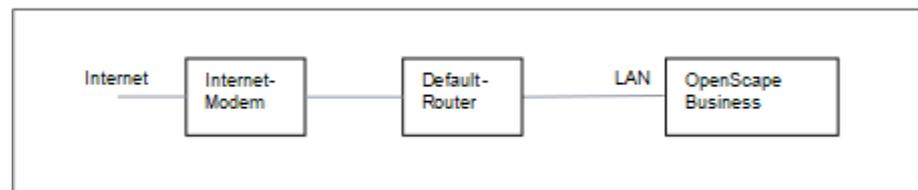
Sie haben folgende Möglichkeiten:

- **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 einen 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.

9.1.2 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.

Anmerkung: 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.

Anmerkung: Für ein Internet-Gespräch werden ca. 128 kbit/s Bandbreite reserviert.

9.1.3 WAN-Schnittstelle

WANs (**Wide Area Network**) werden benutzt, um verschiedene LANs (**Local Area Network**), 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 Internetdienst, 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 Domännennamen (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 Domännennamen 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.

9.2 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

Anmerkung: 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).

Anmerkung: 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 to go und Mobility Entrys](#)).

Kurzbeschreibung:

- Der Mobilfunkbetreiber bietet ein Flatrate-Angebot für das Mobiltelefon an.
- One Number Service: das Mobiltelefon ist unter einer einzigen Festnetzzrufnummer 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 to go ist 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 8 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

Anmerkung: Einrichtebeispiele finden Sie im Internet im **Unify Experts Wiki** unter *OpenScape Business - SIP / ITSP Connectivity - PDF "OSBiz V2 Configuration for ITSP"*.

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 Bereich werden dann manuell als interne Rufnummern der Teilnehmer vergeben.

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	Durchwahl
100	Andreas Richter	897007100

Interne Rufnummer	Name	Durchwahl
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.

Multisite-Management

Die Teilnehmer des Kommunikationssystems können unterschiedlichen Standorten (z.B. mit unterschiedlichen Ortsvorwahlen) zugewiesen werden. Jedem Standort ist eine Richtung und jeder Richtung ist eine ITSP-Registrierung zugeordnet. Es können max. 8 ITSP-Registrierungen verwaltet werden. Dabei ist eine Registrierung pro ITSP möglich oder auch mehrere Registrierungen an einem ITSP. Jeder ITSP-Registrierung kann eine Ortsvorwahl und anschließend mehrere Teilnehmer zugeordnet werden. Der Anschluss der Teilnehmer an den verschiedenen Standorten an das Kommunikationssystem erfolgt über VPN. Alle Standorte müssen sich innerhalb eines Landes befinden und die gleiche Amtskennzahl nutzen (siehe auch *Vernetzung von OpenScape Business in Hosting-Umgebungen*, Szenario 1b).

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.

Leitungsrichtung-Modus

Einzelne Leitungen einer ITSP-Leitung können für ausgehenden und/oder eingehenden Verkehr gesperrt werden. Die folgenden Leitungsrichtung-Modi sind möglich:

- nur gehend
- nur kommend
- Ausgehend und eingehend (Standard)

Die Leitungsrichtung wird ausgewertet, wenn das Kommunikationssystem eine ITSP-Leitung für einen ankommenden oder abgehenden Anruf reservieren muss.

9.2.2 STUN (Simple Traversal of UDP over 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.

Anmerkung: 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.

Anbindung an Service-Provider

Amtszugang über digitale und analoge Leitungen

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
- Ausgehend und eingehend (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.

9.3.2 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.

Tipp: 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 nur B-Kanäle ausgewählt, die in dem Bündel enthalten sind (z.B. über Richtungskennzahl ausgewähltes Bündel, Überlaufbündel oder über LCR ausgewähltes Bündel).

Kommende Gespräche werden immer unabhängig vom Bündel 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 festlegen, nach welchem Kriterium das Kommunikationssystem eine verfügbare Leitung in der entsprechenden Richtung sucht. Die geschieht durch Definition der Belegungsart wie folgt:

- **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 dargestellt 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 Rufnummertyp (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 Rufnummertyp gehend automatisch als führenden Teil der Rufnummer ein. Der Anteil der Anlagenrufnummer muss am Amtsanschluss in Deutschland ohne Ortsnetzkenzahl 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
Ortsnetzkenzahl TON=National	Ortsnetzkenzahl + Anlagenrufnummer + Durchwahlnummer
Ländervorwahl TON=International	Ländervorwahl + Ortsnetzkenzahl + 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.

Rufnummernt zum PSTN übermittelte Rufnummer	
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 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.

9.3.3 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

Wählton je nach Netzbetreiber und Netzzustand variiert, muss das Eintreffen des Wähltons überwacht werden.

Die Konfiguration der Wähltonüberwachungszeit und der Zifferwahlzeit 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.

Anmerkung: 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.

Zifferwahlzeit

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.

Anbindung an Service-Provider

Priorisierung der Amtsholung bei aktiviertem LCR

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.

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)
- UPO-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.

Zugehörige Konzepte

[Lizenzierung](#) auf Seite 150

[Mobility](#) auf Seite 530

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	löschar
Teilnehmer-Durchwahlnummern	11 -30	100-742	löschar
Gruppenrufnummern 1-90 Gruppenrufnummern 91-800	31-40 -	350-439 Nicht vorbelegt	löschar
Leitungsrufnummern	700-703	ab 7801	löschar
Richtungskennzahlen (Externkennzahlen): Rtg. 1 (Amt ISDN, analog) Rtg. 8 (UC Suite) Rtg. 12-15 (Amt ITSP) Rtg. 16 (Vernetzung)	0 = Welt / 9 = USA - Nicht vorbelegt Nicht vorbelegt	0 = Welt / 9 = USA 851 855-858 859	Nur änderbar
Platzkennzahl (Abwurfplatz) Intern	9 = Welt 0 = USA	9 = Welt 0 = USA	Nur änderbar
Platzkennzahl (Abwurfplatz) Durchwahl	0 = Welt - = USA	0 = Welt - = USA	Nur änderbar
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 UC Suite	351 - -	351 Nicht vorbelegt	Nur änderbar Nur änderbar
Konferenz-Rufnummern	-	Nicht vorbelegt	Nur änderbar

Art der Rufnummern	X1	X3/X5/ X8/S	Aktion
Rufnummer für Parken	-	Nicht vorbelegt	Nur änderbar
AutoAttendant-Rufnummern	-	Nicht vorbelegt	Nur änderbar
Rufnummer für Vermittlungsplatz	9 = Welt 0 = USA	9 = Welt 0 = USA	Nur änderbar
Substitution für "#" (bei Servicekennzahlen)	75	75	löschar
Substitution für "#" (bei Servicekennzahlen)	76	76	löschar
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 "löschar" 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

Teilnehmer

Anforderungen an die LAN-Telefonie

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 Datensätze sollten gelöscht werden.
- portdata_xml_import_syntax.txt
Beschreibung in Deutsch und Englisch zum korrekten Anlegen der Datensätze.

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 hängen hierbei von der eingesetzten Netzwerktechnik ab.

Um eine verlustfreie Übertragung und eine gute Sprachqualität zu gewährleisten, werden die Sprachsignale mit Hilfe von Audio-Codern 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-Codern

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-Codexs

Folgende Audio-Codexs 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-Codexs 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 Codexs 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-Codexs zu deaktivieren und nur die G.711-Codexs zu verwenden. Damit wird die Anzahl der möglichen, parallel geführten Gespräche optimiert. Wird diese Funktion aktiviert, ist ein Neustart des Systems nötig.

In OSBiz X-Systemen gibt es kein End-to-End Payload zwischen Circuit- und HFA-Benutzern. Die Payload endet im System, sodass die Benutzer mit einem Codec sprechen, der vom System unterstützt wird. Das HFA-Telefon hat beispielsweise zunächst den Codec G.722 eingestellt und der Circuit-Benutzer unterstützt G.722. Das System unterstützt den G.722-Codec nicht und der G.711-Codec wurde als erste Option festgelegt. In diesem Fall sprechen beide Benutzer mit dem G.711-Codec. Bei OSBiz S-Systemen sprechen die Benutzer mit dem G.722-Codec, solange ein End-to-End Payload vorhanden ist.

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.

10.2.3 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 Kommunikationssystems 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
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)

10.3 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.

IP-Teilnehmer konfigurieren

Folgende Konfigurationen zu einem IP-Teilnehmer können durchgeführt werden:

- Konfiguration der Standard-Parameter mit dem Wizard **IP-Endgeräte** (siehe [IP-Teilnehmer konfigurieren](#)).
- Konfiguration aller Parameter (Standard-Parameter und erweiterte Parameter) über den Experten-Modus (siehe [>Station>Station>IP Clients](#)).

OpenScape Desk Phone IP Systemtelefone werden standardmäßig mit der SIP-Software ausgeliefert. Sobald ein OpenScape Desk Phone IP Systemtelefon im WBM als **System Client** konfiguriert wird, wird automatisch die im Kommunikationssystem gespeicherte HFA-Software auf das IP-Systemtelefon geladen.

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: vorgelegt, kann bei Bedarf geändert werden, max. 20 Zeichen. Jeder SIP-Teilnehmer hat eine andere vorgelegte SIP User ID.

- Realm

Zone oder Domäne für die Authentifizierung: vorgelegt, kann bei Bedarf geändert werden, max. 20 Zeichen. Der Realm ist für alle SIP-Teilnehmer mit dem gleichen Wert vorgelegt. 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 Assistenten **IP-Endgeräte** (siehe [So konfigurieren Sie SIP-Teilnehmer](#)).
- 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)

Anmerkung: Der Einsatz mit Multichannel Contact Center ist nicht freigegeben (z. B. Übergabe an UCD-Gruppen).

Je nach Telefon können sich Einschränkungen der verfügbaren Funktionen ergeben, siehe Wiki unter: http://wiki.unify.com/wiki/SIP_devices_configuration_examples

Folgende Leistungsmerkmale, die durch Kennzahlen mit * oder # aktiviert werden, können mit SIP-Telefonen genutzt werden:

- Dienste 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
- Anruf halten
- Makeln
- Rückfrage
- Trennen
- Übergeben

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 [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 X1W/X3W/X3R/X5R
Cordless-Basisstation an eine UP0/E-Schnittstelle des Mainboards.
- OpenScape Business X8
Cordless-Basisstation an eine oder mehrere SLMUC-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 Assistenten **DECT-Endgeräte** (siehe [So konfigurieren Sie DECT-Teilnehmer](#)).
- Konfiguration aller Parameter (Standard-Parameter und erweiterte Parameter) über den Experten-Modus (siehe [Teilnehmer>Teilnehmer>DECTTeilnehmer>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 S₀-Bus. Deshalb wird er auch oft S₀-Teilnehmer genannt. Mit dem Kommunikationssystem wird der ISDN-Teilnehmer über die S₀-Schnittstellen verbunden.

Für einen S₀-Teilnehmer gibt es folgende Anschlussmöglichkeiten:

- OpenScape Business X1
an eine S₀-Schnittstelle des Mainboards.
- OpenScape Business X3/X5
an eine S₀-Schnittstelle des Mainboards oder an eine S₀-Baugruppe.
- OpenScape Business X8
an eine oder mehrere S₀-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 S₀-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 S₀-Schnittstelle

Um ISDN-Teilnehmer an das Kommunikationssystem anschließen zu können, muss mindestens eine der S₀-Schnittstellen, die für den ISDN-Teilnehmeranschluss oder den ISDN-Anlagenanschluss verwendet werden, als interner S₀-Bus (S₀-Euro-Bus) konfiguriert werden.

Anmerkung: Falls bei einem ISDN-Mehrgeräteanschluss mehrere ISDN-Teilnehmer an einer S₀-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 [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 hinzuzufügen, 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 S₀-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.

10.8 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 [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 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 Ebenenumschalttaste (Shift-key) eingerichtet sein. Die LEDs der Funktionstasten gehört dabei immer zur 1. Ebene.

Anmerkung: Bei einem **Benutzer kann die Tastenprogrammierung nicht kopiert werden, da die Funktion der automatischen Tastenbelegung MULAP-spezifisch ist und in keinem Fall kopiert werden sollte. Das Präfix ** sollte manuell von diesen Benutzern entfernt werden, damit das Kopieren der Tastenbelegung aktiviert werden kann.

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. Zusätzliche Einstellungen (wie z.B. die Rufsignalisierung oder die Teilnehmer-Flags) können für jeden Teilnehmer einzeln geändert werden.

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.

- **Fax-Rufnummer, Fax-Durchwahlnummer**

Wenn für den Teilnehmer eine Faxbox eingerichtet werden soll (nutzbar z.B. mit den UC Clients myPortal for Desktop oder myPortal for Outlook) vergeben Sie eine Fax-Rufnummer (für den Empfang interner Faxnachrichten) und eine Fax-Durchwahlnummer (für den Empfang externer Faxnachrichten).

- **Berechtigungen (Classes of Service)**

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 \(Wahlkontrolle\)](#)).

- **Anrufübernahmegruppe**

Jeder Teilnehmer kann einer Anrufübernahmegruppe zugeordnet werden.

- **Sprache, Rufsignalisierung**

Die Sprache für die Menüsteuerung der angeschlossenen Systemtelefone kann eingestellt 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 \(SmartVM\)](#)

Bei der UC-Lösung UC Suite wird jedem Teilnehmer automatisch eine Sprachbox zugewiesen. Somit fehlen in diesem Fall die Sprachbox-Einstellungen.

- **Teilnehmer-Flags**

Die Teilnehmer-Flags eines jeden Teilnehmers können geändert werden. Für eine Beschreibung der Teilnehmer-Flags siehe [>Teilnehmer>Teilnehmer>Teilnehmer-Parameter](#).

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

Teilnehmer

Konfiguration der Teilnehmer-Profile

müssen nur im Bedarfsfall angepasst werden. Informationen zu den erweiterten Einstellungen siehe [Teilnehmer](#).

Zugehörige Konzepte

[Berechtigungen \(Wahlkontrolle\)](#) auf Seite 410

[Mehrsprachige Textausgabe](#) auf Seite 701

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.

10.14 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):

- Passwort
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.

10.15 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**.

11 UC Smart

UC Smart ist in allen OpenScape Business Modellen (mit und ohne UC Booster) integriert und bietet Unified Communications Leistungsmerkmale wie z.B. Anwesenheitsstatus und Sprachnachrichten sowie zusätzlich Konferenzen.

Clients für UC Smart

Die UC Smart Funktionen können mit folgenden Clients genutzt werden:

- myPortal @work
- myPortal to go (als Mobile UC App oder als Web Edition)
- Application Launcher
- OpenScape Business Attendant / BLF
- 3rd Party WSI Clients

Die Ausbaugrenzen sind abhängig vom genutzten OpenScape Business Modell und von den ggf. installierten OpenScape Business UC Booster Varianten.

Besonderheiten von UC Smart bei OpenScape Business S

Bedingt durch die Systemarchitektur gibt es bei OpenScape Business S folgende Einschränkungen:

- Die Anzahl der Voicemail-Nachrichten wird nicht im Display des Telefons angezeigt (MWI).
- Bei der Sprachbox (SmartVM) wird keine Fax,- Besetzt,- oder Ruheerkennung unterstützt. Kommende Fax-Verbindungen können nach Rufannahme durch die SmartVM nicht zu einem Standard-Fax-Gerät vermittelt werden. Die SmartVM zeichnet für 2 Minuten auf.
- Bei Vermittlung von Verbindungen durch den Company AutoAttendant auf besetzte Teilnehmer erhält der Anrufer Besetztton. Es besteht keine Möglichkeit eine Sprachnachricht zu hinterlassen.
- Soll bei der Abfrage einer Sprachnachricht auf die in der SmartVM hinterlegte Rufnummer weitergeleitet werden (Calling Party Number), muss diese Rufnummer identisch sein mit der für die SmartVM konfigurierten Rufnummer des Benutzers.
- Bei Verbindungen zur Sprachbox (SmartVM) werden beim UC Booster Server und bei OpenScape Business S SIPQ-Trunks belegt. Dafür werden keine Trunk-Lizenzen benötigt.
- Für gleichzeitige Ansagen werden MEB-Kanäle belegt.
- Für Sprachverbindungen zur Sprachbox (SmartVM) oder AutoAttendant stehen sechzig MEB-Kanäle zur Verfügung.

Anmerkung: Nach Änderungen in der Konfiguration von Stationen, Gruppen, Mobility oder anderen Systemparametern wie Trunk Access Codes müssen die UC-Daten für UC Smart oder UC Suite synchronisiert werden. Die Synchronisation erfolgt fünf Minuten nach der letzten Konfigurationsänderung. Wenn eine spätere Konfigurationsänderung vor dem 5-Minuten-Timer

erfolgt, wird der Timer neu gestartet. UC-Daten können veraltet sein, bis die Synchronisation beginnt.

Zugehörige Konzepte

[UC-Funktionen \(Überblick\)](#) auf Seite 50

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 Initial-Kennwort vergeben und dieses Kennwort den Benutzern mitteilen. Das Initial-Kennwort kann für alle Benutzer gleich sein oder für jeden Benutzer unterschiedlich. Das 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.

Erweiterte Einstellungen für applikationsgesteuerte Konferenzen (optional)

Der Administrator muss im WBM während der Grundinstallation die **Funktionskennzahl für MeetMe Konferenz** (MeetMe-Einwahlnummer) und mindestens eine **Funktionskennzahl für Konferenz** (Konferenzraum) einrichten.

Für OpenScape Business X Systeme muss der MeetMe-Einwahlnummer eine Rufzielliste zugewiesen werden, in der der erste Eintrag leer ist und der zweite Eintrag der Rufnummer der Sprachbox (SmartVM) entspricht.

Für OpenScape Business S Systeme muss der MeetMe-Einwahlnummer eine Rufzielliste zugewiesen werden, in der der erste Eintrag der Rufnummer der Sprachbox (Richtung Anwendungssuite).

Zuletzt muss der MeetMe-Einwahlnummer noch eine Standardmailbox zugeordnet werden.

Die Beschreibung der Konfiguration finden Sie hier: [Wie Sie die applikationsgesteuerten Konferenzen konfigurieren](#),

Lizenzzuweisungen

Der Administrator muss jedem UC Smart User eine UC User-Lizenz zuweisen.

Optional können zusätzliche Lizenzen zugewiesen werden für:

- Voicemail (auch ohne UC Smart nutzbar)
- Konferenz

- Application Launcher

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 @work	PC
Mobile Client	myPortal to go (UC Smart) (siehe Mobility auf Seite 530)	Smartphone, Tablet-PC
Communications Client	OpenScape Desk Phone CP 400/600/600E/ 700/700X/710 HFA (in der Telefon-Software integrierter Client)	OpenScape Desk Phone CP 400/600/600E/ 700/700X/710 HFA

11.2.1 myPortal @work

myPortal @work ist eine Unified-Communication-Anwendung (Microsoft Windows und Mac OS X), die alle benötigten Funktionen und Services wie komfortables Wählen über Telefonverzeichnisse, Favoriten, Gespräche und Informationen zum Anwesenheitsstatus von Kollegen zu einem zentralen Lösungskonzept vereint, um die tägliche Kommunikation zu beschleunigen, die Teamarbeit zu verbessern sowie rasch mit Kollegen, Kunden und Partnern in Verbindung zu treten.

myPortal @work kann entweder im UC Smart oder im UC Suite Modus verwendet werden. Je nach Modus variieren die angebotenen Funktionen in der Benutzeroberfläche. Sie können die Betriebsart nicht ändern, da dies durch den Systemadministrator festgelegt ist. Wenn Sie Zweifel an der aktuellen Betriebsart Ihres myPortal @work-Clients haben, fragen Sie Ihren Systemadministrator um Rat.

myPortal @work bietet einen integrierten Voice over IP (VoIP) Telefonie-Client. Wenn die Option VoIP aktiviert ist, nutzen die sprachbezogenen Funktionen des myPortal @work-Clients die VoIP-Funktionen.

Anmerkung: Um die Voice over IP (VoIP)-Funktionen nutzen zu können, muss der Benutzer als System-Client konfiguriert sein.

Infos zur remoten Verwendung von VoIP über Device@Home, siehe [1 Konfiguration für System Device@Home](#)

Die VoIP-Funktionen unterstützen eine Reihe von Funktionen, die über die UC-Funktionen hinausgehen:

- Anrufen
- Anruf annehmen
- Anruf beenden
- Rückfrage
- Übergeben nach Melden
- Übergabe ohne Rückfrage
- Ruf abweisen
- Zur Voicemail umleiten
- Wiederanruf (Benachrichtigung für einen Wiederanruf anzeigen wird noch nicht unterstützt)
- Makeln
- Stumm/Stummschalten aufheben(nur für VoIP-Funktionen)
- Systemkonferenz
- Anklopfschutz
- Sie klopfen an
- Anrufschutz (DND)
- DTMF
- Anrufübernahme

Anmerkung: Da der myPortal@Work-Client die Fähigkeit, DTMF-Töne an eine andere Station zu senden, nicht unterstützt, wird das Senden eines DTMF-Tons über den CSTA-Befehl „generateDigits“ ebenfalls nicht unterstützt, und eine solche Anfrage wird vom System abgelehnt und zurückgewiesen.

Arbeiten im Team:

myPortal @work VoIP-Client kann auch verwendet werden in:

- Gruppe (z. B. Linear, Anklopfen)
- MULAP als MULAP-Mitglied

Signaling- und Payload-Encryption (SPE) wird für das Kommunikationssystem ebenfalls unterstützt. Der VoIP-Client verwendet einen modernen WebRTC-Sicherheitsstapel und bietet somit auch einen sicheren Datentransfer mittels DTLS.

Anmerkung: Die Konfiguration von ITSP SDES wird ebenfalls unterstützt.

Servicecodes können über die Suchleiste verwendet werden, werden aber bei Problemen nicht unterstützt. Rückmeldungen über die erfolgreiche oder erfolglose Ausführung von Servicecodes werden nicht ausgegeben und es wird daher dringend empfohlen, die Eingabemöglichkeiten der Benutzeroberfläche myPortal @work zu nutzen, um die jeweiligen Funktionen zu steuern.

myPortal @work im UC Suite Modus kann nicht nur eigenständig, sondern auch in Verbindung mit dem bestehenden myPortal for Desktop/Outlook, myAgent, myAttendant Client (CTI, Favoriten und

Gespräche) genutzt werden. Die vorhandenen UC User-Lizenzen können auch mit myPortal @work verwendet werden.

Die folgenden Abbildungen zeigen überwiegend myPortal @work im UC Smart Modus. Auf Abweichungen im UC Suite Modus wird ausdrücklich im Benutzerhandbuch für myPortal @work hingewiesen.

myPortal @work unterstützt allgemein folgende Leistungsmerkmale:

- Anwesenheitsstatus
- Statusbezogene Anrufumleitung
- Verzeichnisse einschließlich Suchen nach Namen
- Favoriten
- Konversationen: bis zu 25 Konversationen werden im Client angezeigt und jede Konversation hat bis zu 50 Einträge
- Konferenzschaltung
- Hotkey-Wahl/Hotkey-Suche/Telefonie-Hyperlinks
- Anruffunktionen über:
 - 1) Zugewiesenes Telefon
 - 2) Integrierten Voice over IP Telefonie-Client
- Voicemail-Steuerung
- Vergrößern/Verkleinern
- Bildschirmteilung mittels OpenScape Web Collaboration (optional)

Verwendung von myPortal @work in einer Microsoft Terminal Server-Umgebung

myPortal @work wurde für UC- und CTI-Funktionen in Microsoft Terminal Server-Umgebungen mit den folgenden Einschränkungen freigegeben:

- Telefonie-Hyperlinks und Click-to-Dial werden nicht unterstützt
- Anwendungsstart beim Hochfahren wird nicht unterstützt
- Hochladen von Benutzerbildern wird nicht unterstützt
- Die Funktionen für Andocken/Abdocken, Anheften/Loslösen und Minimieren auf der Taskleiste sind begrenzt
- Die Funktion VoIP wird nicht unterstützt

11.2.1.1 Voraussetzungen für myPortal @work

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.

Die folgenden Voraussetzungen sind für die Installation von myPortal @work nötig:

- Administratorrechte
- myPortal @work Software-Einrichtungsprogramm
- IP-Adressen und Ports des Kommunikationssystems
- FQDN oder IP-Adresse, Port für WAN-Verbindung (Gerät@home)

- Zugangsdaten (Benutzer und Kennwort) für Ihr UC-Benutzerkonto im Kommunikationssystem
- Sprachbox-Kontoinformationen (optional)
- MULAP-Rufnummer bei mehrfacher Nummernvergabe (optional)
- Windows OS und Apple Mac OS X

Anmerkung: TLS 1.2 muss unter Internetoptionen (in der Systemsteuerung) aktiviert sein und die neuesten Patches von Microsoft müssen manuell installiert bzw. aktiviert werden.

Wenn die genannten Aktionen nicht ausgeführt werden, wird der HTTPS-Zugriff abgelehnt.

Telefone

myPortal @work kann in Verbindung mit folgenden Telefonen genutzt werden:

Anmerkung: myPortal @work kann auch einzeln mit VoIP-Funktionen verwendet werden, ohne ein physisches Gerät zu verwenden.

- OpenStage HFA
- OpenScape Desk Phone IP 35G/55G HFA
- OpenScape Desk Phone IP 35G Eco HFA
- OpenScape Desk Phone CP 100/200/205/400/600/600E/700/700X HFA
- OpenScape Desk Phone CP 110/210/710 HFA
- Analoge Telefone
- ISDN-Telefone
- OpenScape Personal Edition HFA
- OpenStage M3 (OpenScape Business Cordless)
- OpenScape DECT Phone S6/SL6/R6 (OpenScape Business Cordless)

Ältere Geräte (z. B. optiPoint 410/420/500 und Gigaset M2/SL3/S4/SL4/S5) werden unterstützt. Optiset E-Geräte können nicht betrieben werden. Getestete und freigegebene Geräte entnehmen Sie bitte der Freigabemitteilung.

Anmerkung: Für den in OpenScape Desk Phone CP 400/600/600E/700/700X/710 HFA integrierten Client gelten außer der Standard-Client-Konfiguration und -Lizenz keine besonderen Voraussetzungen.

"Favoriten" im Telefonmenü enthält frei programmierbare Tasten und bezieht sich nicht auf UC-Favoriten. Details zu diesen Schlüsseln und eine Anleitung dazu finden Sie in der Gerätedokumentation.

Anmerkung: Bei analogen Telefonen und DECT-Telefonen wird die Message Waiting Indication (MWI)

nicht unterstützt, die Anzeige von Informationen im Display wird nur eingeschränkt unterstützt.

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)
- Google Chrome

Installationsdateien

Der Administrator kann die Installationsdateien aus dem **Service-Center > Software** herunterladen und diese den Benutzern bereitstellen, z. B. über ein Netzlaufwerk.

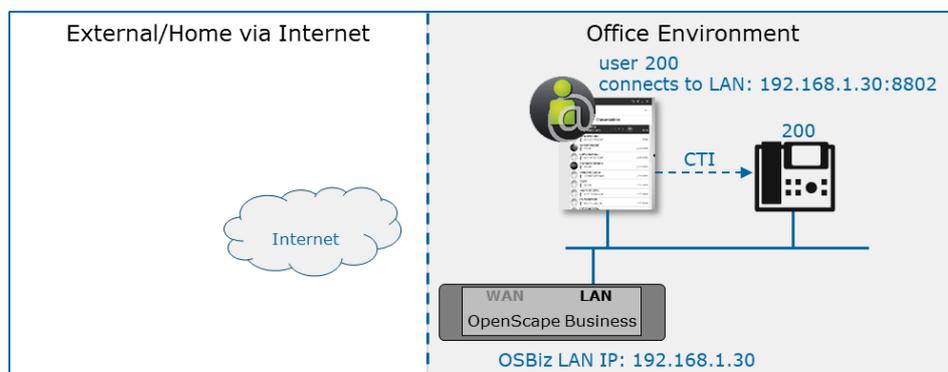
11.2.1.2 myPortal@work: Benutzerkonfiguration

myPortal @work ist eine Kombination aus UC- und VoIP-Client, und diese beiden Funktionalitäten erfordern die folgenden Konfigurationen/Lizenzen für verschiedene UC-Modi (Smart/UC Suite) und Anwendungsfälle.

Anmerkung: Wenn ein myPortal @work-Benutzerkonto nach mehreren fehlerhaften Anmeldeversuchen im UC Suite-Modus gesperrt wird, ist es im UC Suite-Benutzerverzeichnis nicht sichtbar. Sie können die gesperrten myPortal @work-Benutzer unter **Expertenmodus > Web Services > Web Services Assistant > Benutzerverwaltung** einsehen, diese Konten lassen sich jedoch unter **Expertenmodus > OpenScape Business UC Suite > Benutzerverzeichnis** wieder entsperren.

Lokale LAN-Konfiguration - nur UC- und CTI-Client

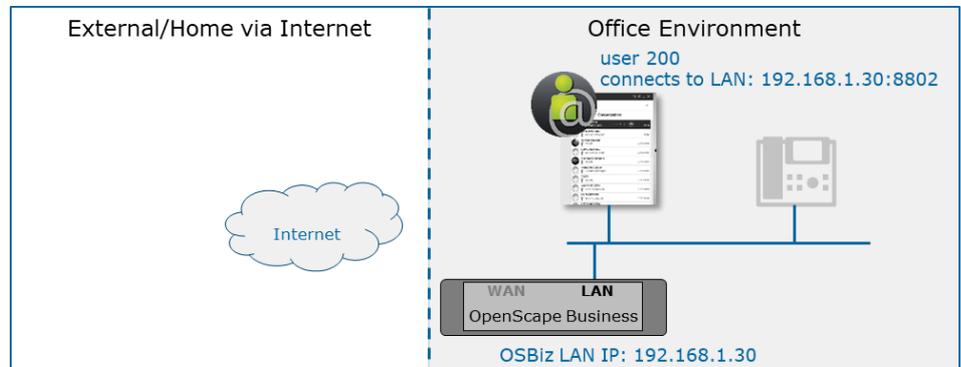
myPortal @work wird als UC- und CTI-Client für ein angeschlossenes Tischtelefon ohne VoIP verwendet.



- Lizenzen: UC User oder Groupware User

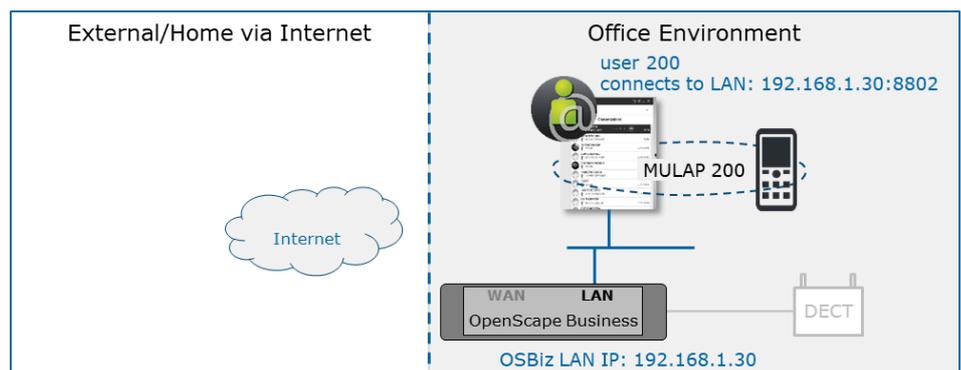
- myPortal @work Anmeldung: Geben Sie im Anmeldebildschirm Ihren Benutzernamen und Ihr Kennwort sowie LAN IP-Adresse:8802 ein.

Lokale LAN-Konfiguration – UC- und VoIP-Client



- Lizenzen: IP User- und UC User- oder Groupware-Lizenz
- myPortal @work Anmeldung: Geben Sie im Anmeldebildschirm Ihren Benutzernamen und Ihr Kennwort sowie LAN IP-Adresse:8802 ein.
- myPortal @work VoIP-Registrierung: Nachdem Sie sich erfolgreich angemeldet haben, müssen Sie zu Einstellungen > VoIP > VoIP aktivieren gehen
- STUN-Konnektivität im Client ist für reine Inhouse-Verbindungen nicht erforderlich. Diese wird jedoch in einigen hybriden Szenarien gebraucht, die myPortal @work VoIP über das öffentliche Internet nutzen. Zum Prüfen der STUN-Konnektivität gehen Sie zu Einstellungen > VoIP > Erweiterte ICE-Einstellungen > ICE-Status prüfen.

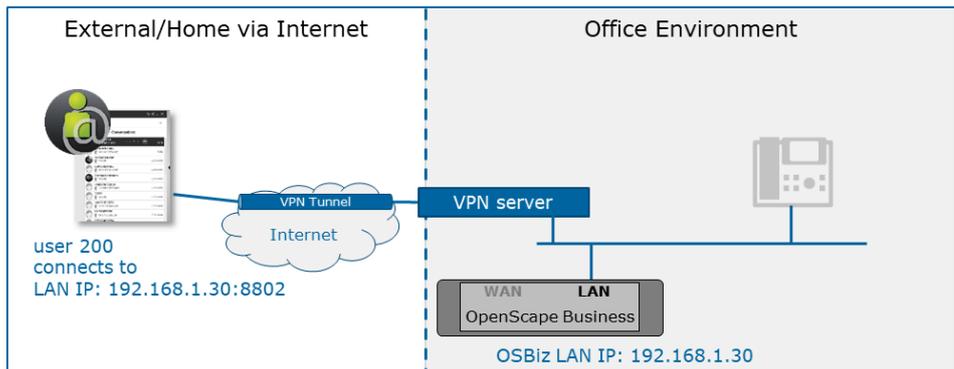
MULAP-Benutzerkonfiguration (Lokales LAN)



- Lizenzen:
 - myPortal @work: IP User- und UC User- oder Groupware-Lizenz
 - ein anderes MULAP-Gerät - in diesem Beispiel DECT: TDM-Benutzerlizenz oder IP-Benutzer (Die MULAP-Konfiguration wird für die Kombination mit TDM- oder DECT-Geräten empfohlen, kann aber auch mit einem IP-Gerät verwendet werden.)
- myPortal @work Anmeldung: Geben Sie im Anmeldebildschirm Ihren Benutzernamen und Ihr Kennwort sowie die MULAP-Nummer / LAN IP-Adresse:8802 ein.

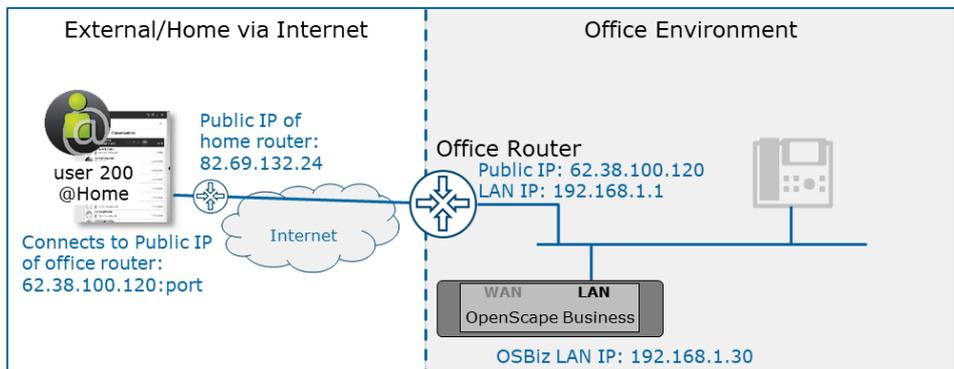
- myPortal @work VoIP-Registrierung: Nachdem Sie sich erfolgreich angemeldet haben, müssen Sie zu Einstellungen > VoIP gehen, das gesteuerte Gerät auswählen und dann VoIP aktivieren
- STUN-Konnektivität im Client ist für reine Inhouse-Verbindungen nicht erforderlich. Dennoch ist dies in einigen hybriden Szenarien mit anderen Benutzern erforderlich, die myPortal @work VoIP über das öffentliche Internet nutzen. Zum Prüfen der STUN-Konnektivität gehen Sie zu **Einstellungen > VoIP > Erweiterte ICE-Einstellungen > ICE-Status prüfen**.

Heimwender mit VPN-Verbindungskonfiguration



- Lizenzen: IP User- und UC User- oder Groupware-Lizenz
- myPortal @work Anmeldung: Geben Sie im Anmeldebildschirm Ihren Benutzernamen und Ihr Kennwort sowie LAN IP-Adresse:8802 ein.
- myPortal @work VoIP-Registrierung: Nachdem Sie sich erfolgreich angemeldet haben, müssen Sie zu Einstellungen> VoIP> VoIP aktivieren gehen
- STUN-Konnektivität ist obligatorisch. Zum Prüfen der STUN-Konnektivität gehen Sie zu Einstellungen > VoIP > Erweiterte ICE-Einstellungen > ICE-Status prüfen.

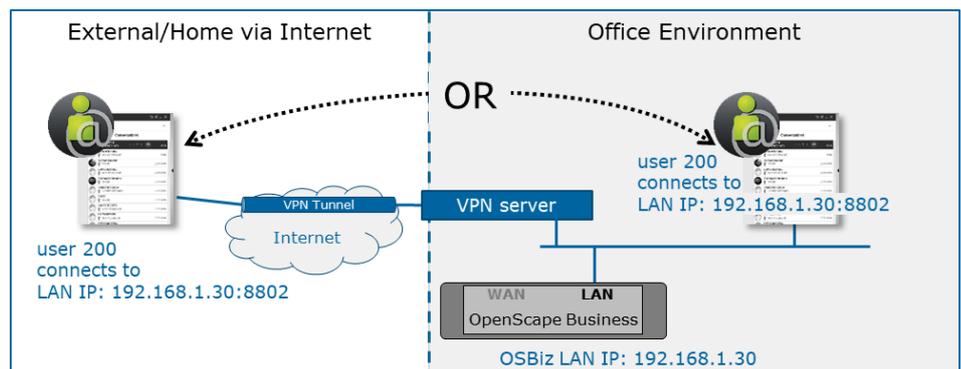
myPortal @work über das öffentliche Internet



- Lizenzen: IP User- und UC User- oder Groupware-Lizenz
- myPortal @work login: Geben Sie im Anmeldebildschirm Ihren Login-Benutzernamen/Kennwort / öffentliche IP-Adresse:Port ein, die sie vom Administrator erhalten haben.

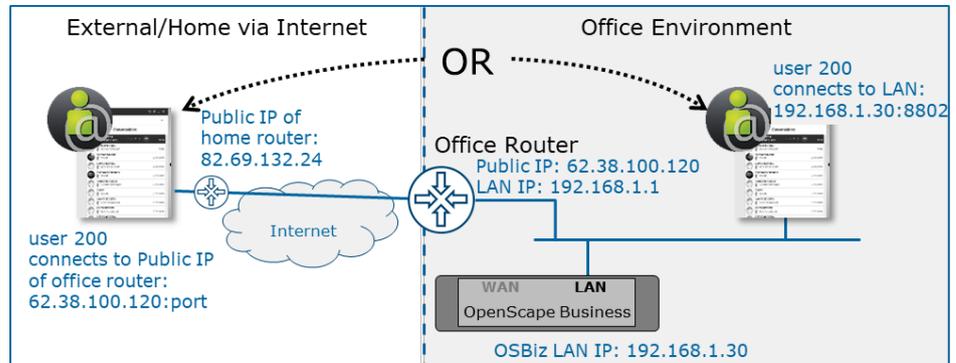
- myPortal @work VoIP-Registrierung: Nachdem Sie sich erfolgreich angemeldet haben, müssen Sie zu Einstellungen > VoIP > VoIP aktivieren gehen
- Bereiten Sie die Netzwerkumgebung vor, siehe Kapitel [Konfigurationsschritte zur Nutzung von myPortal @work über das Internet](#) auf Seite 243
- Das SBC-Flag ist für myPortal @work nicht erforderlich. Es wird nur gebraucht, wenn Sie ein Hardwaregerät verwenden.
- Bitte nicht die OSBiz WAN-Schnittstelle für die Verbindung zum Internet verwenden, wenn Sie myPortal @work über Public IP nutzen. In diesem Fall erkennt der interne SBC die öffentliche IP-Adresse der WAN-Schnittstelle und nutzt diese für die Kommunikation zwischen Client und OSBiz, was zu Problemen mit der Nutzlast führt. Vorgeschlagene Konfiguration: Verbinden Sie das ISTP über die LAN-Schnittstelle. Dies kann über den normalen ISP-Router oder über einen zweiten Router und statische Routen erfolgen.
- STUN-Konnektivität ist erforderlich. Zum Prüfen der STUN-Konnektivität gehen Sie zu Einstellungen > VoIP > Erweiterte ICE-Einstellungen > ICE-Status prüfen.

Heimanwender mit VPN und lokaler LAN-Konfiguration (z. B. beim Wechsel vom Büro nach Hause und zurück)



- Lizenzen: IP User- und UC User- oder Groupware-Lizenz
- myPortal @work Anmeldung: Geben Sie im Anmeldebildschirm Ihren Benutzernamen und Ihr Kennwort sowie LAN IP-Adresse:8802 ein.
- myPortal @work VoIP-Registrierung: Nachdem Sie sich erfolgreich angemeldet haben, müssen Sie zu Einstellungen > VoIP > VoIP aktivieren gehen
- myPortal @work kann in beiden Umgebungen ohne Ändern der Einstellungen verwendet werden.
- STUN-Konnektivität ist zwingend erforderlich. Zum Prüfen der STUN-Konnektivität gehen Sie zu Einstellungen > VoIP > Erweiterte ICE-Einstellungen > ICE-Status prüfen.

myPortal @work über das öffentliche Internet und die lokale LAN-Konfiguration (z. B. beim Wechsel vom Büro nach Hause und zurück)



- Lizenzen: IP User- und UC User- oder Groupware-Lizenz
- Anmeldung bei myPortal @work: Geben Sie im Anmeldebildschirm Ihren Login-Benutzernamen/Kennwort und die vom Administrator konfigurierte LAN-IP-Adresse:8802 und öffentliche IP-Adresse:Port ein. Wenn Sie beide Adressen konfigurieren, müssen Sie kein zweites Profil verwenden, wenn Sie vom Büro nach Hause und zurück wechseln.
- myPortal @work VoIP-Registrierung: Nachdem Sie sich erfolgreich angemeldet haben, müssen Sie zu Einstellungen> VoIP> VoIP aktivieren gehen
- Bereiten Sie die Netzwerkumgebung vor, siehe Kapitel [Konfigurationsschritte zur Nutzung von myPortal @work über das Internet](#) auf Seite 243
- Das SBC-Flag ist für myPortal@work nicht erforderlich. Es wird nur gebraucht, wenn Sie ein Hardwaregerät verwenden.

Für die VoIP-Registrierung

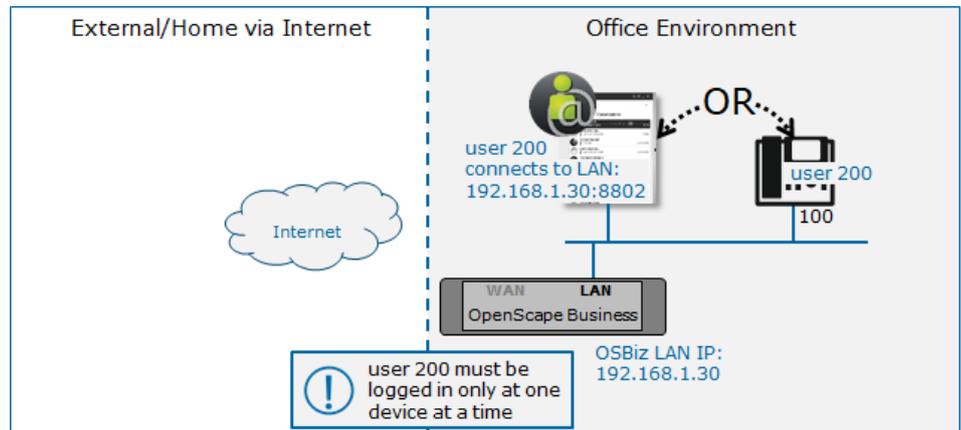
Wenn sowohl lokale als auch Heimanwender verwendet werden, sollte der Anwender nur einen VoIP-Anschluss entweder zu Hause oder im Büro haben.

Für UC

Wenn der Anwender an mehreren Orten gleichzeitig mit UC verbunden sein möchte:

- UC Smart Modus: UC-Clients können gleichzeitig von zu Hause und vom Büro aus verbunden sein, aber in diesem Szenario wird nur ein VoIP-Client unterstützt, und die VoIP-Funktionalität des anderen Clients sollte unregistriert bleiben.
- UC Suite Modus: Bitte prüfen Sie den Abschnitt „Kombination von myPortal @work mit anderen UC Suite-Clients und Lizenzkonfiguration“. Es ist nur ein myPortal @work Client erlaubt.

Deskshare-Benutzer über lokales LAN

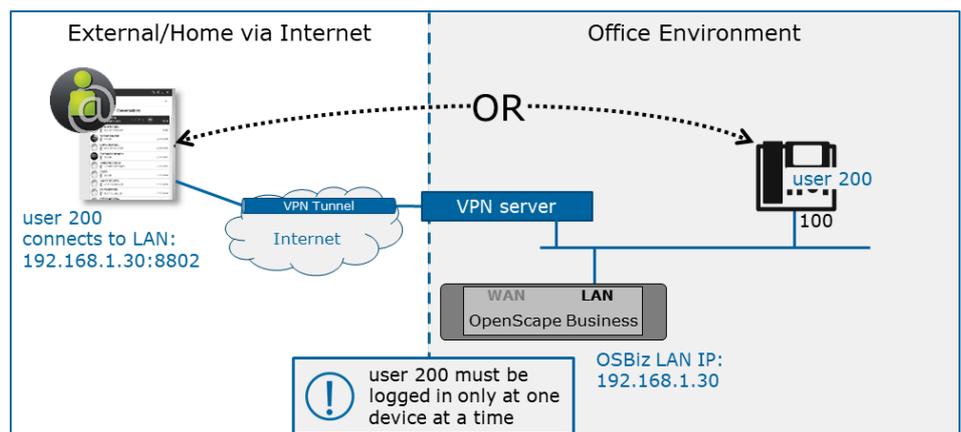


- Lizenzen: Deskshare-Lizenz and UC User- oder Groupware-Lizenz
- myPortal @work login: Geben Sie im Anmeldebildschirm die Anmeldung der Deskshare-Erweiterung Benutzername/Kennwort/ LAN-IP-Adresse:8802 ein.
- myPortal @work VoIP-Registrierung: Nachdem Sie sich erfolgreich angemeldet haben, müssen Sie zu Einstellungen> VoIP> VoIP aktivieren gehen

Beispiel: Gerät nutzt Dummy-Nummer = „100“. Verbinden Sie sich mit Ihrem DeskPhone als Deskshare mit „100“, z. B. 200 mit Servicecode *9419.

Um myPortal @work mit Benutzer 200 zu nutzen, wird das Deskphone automatisch abgemeldet und kehrt zur Dummy-Nummer „100“ zurück. Wenn Sie wieder zum Deskphone wechseln, ist sicherzustellen, dass myPortal @work nicht registriert ist (der Benutzer muss die Anwendung beenden oder sich abmelden).

Externer Deskshare-Benutzer über VPN



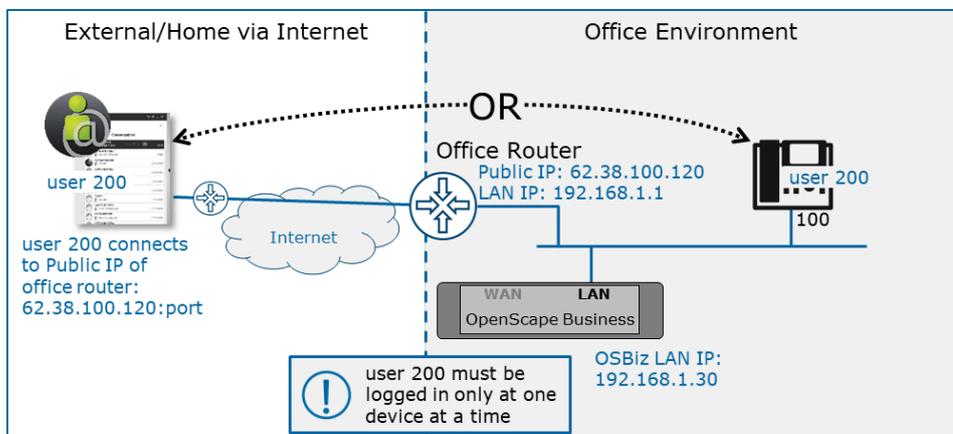
- Lizenzen: Deskshare-Lizenz and UC User- oder Groupware-Lizenz
- myPortal @work login: Geben Sie im Anmeldebildschirm die Anmeldung der Deskshare-Erweiterung Benutzername/Kennwort/ LAN-IP-Adresse:8802 ein.

- myPortal @work VoIP-Registrierung: Nachdem Sie sich erfolgreich angemeldet haben, müssen Sie zu Einstellungen> VoIP> VoIP aktivieren gehen

Beispiel: Gerät nutzt Dummy-Nummer = „100“. Verbinden Sie sich mit Ihrem DeskPhone als Deskshare mit „100“, z. B. 200 mit Servicecode *9419.

Um myPortal @work mit Benutzer 200 zu nutzen, wird das Deskphone automatisch abgemeldet und kehrt zur Dummy-Nummer „100“ zurück. Wenn Sie wieder zum Deskphone wechseln, ist sicherzustellen, dass myPortal @work nicht registriert ist (der Benutzer muss die Anwendung beenden oder sich abmelden).

Externer Deskshare-Benutzer über das öffentliche Internet



- Lizenzen: Deskshare-Lizenz and UC User- oder Groupware-Lizenz
- myPortal @work login: Geben Sie im Anmeldebildschirm die Anmeldung der Deskshare-Erweiterung Benutzername/Kennwort/ LAN-IP-Adresse:8802 ein.
- myPortal @work VoIP-Registrierung: Nachdem Sie sich erfolgreich angemeldet haben, müssen Sie zu Einstellungen> VoIP> VoIP aktivieren gehen

Beispiel: Gerät nutzt Dummy-Nummer = „100“. Verbinden Sie sich mit Ihrem DeskPhone als Deskshare mit „100“, z. B. 200 mit Servicecode *9419.

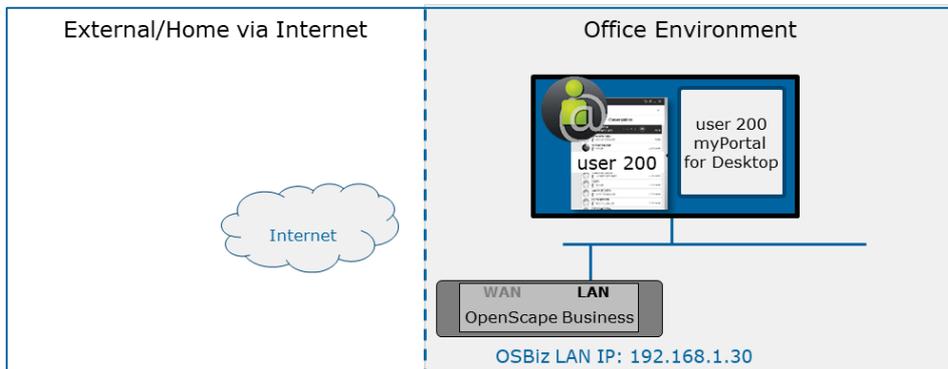
Um myPortal @work mit Benutzer 200 zu nutzen, wird das Deskphone automatisch abgemeldet und kehrt zur Dummy-Nummer „100“ zurück. Wenn Sie wieder zum Deskphone wechseln, ist sicherzustellen, dass myPortal @work nicht registriert ist (der Benutzer muss die Anwendung beenden oder sich abmelden).

Kombination von myPortal @work mit anderen UC Suite-Clients und Lizenzkonfiguration

Anmerkung: Die in diesem Kapitel beschriebenen Konfigurationen werden auch für Heimanwender über VPN unterstützt.

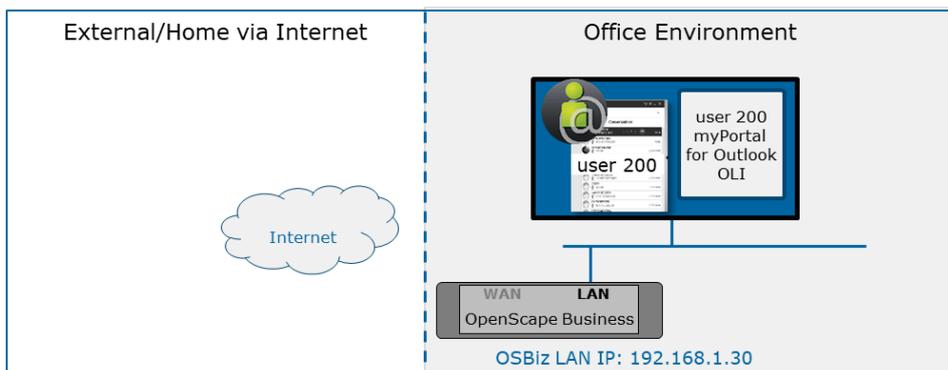
UC User-Lizenz

Derselbe Benutzer kann parallel mit myPortal @work und myPortal for Desktop verbunden sein.



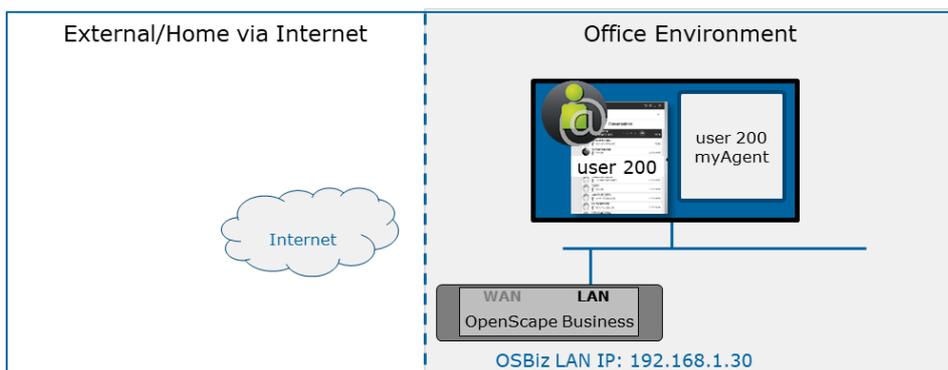
Groupware-Lizenz

Derselbe Benutzer kann parallel mit myPortal @work und OLI verbunden sein.



Kombination aus IP-, UC User- und myAgent-Lizenz

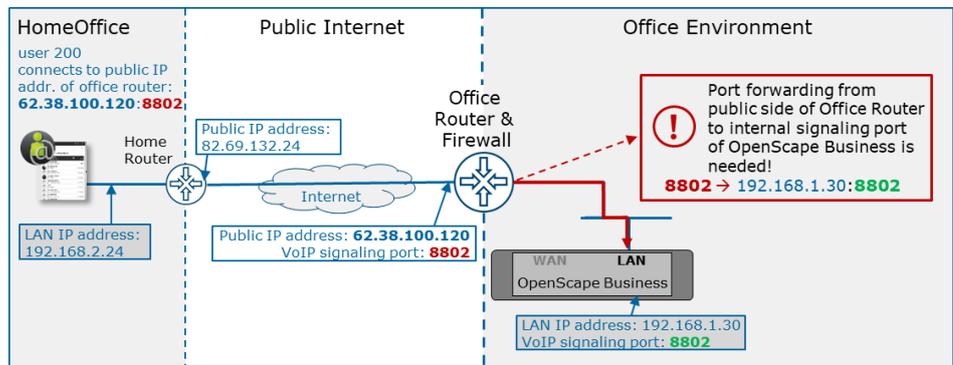
myAgent und myPortal @work VoIP lassen sich parallel als Softphone nutzen.



11.2.1.3 Konfigurationsschritte zur Nutzung von myPortal @work über das Internet

Um myPortal @work über das Internet nutzen zu können, muss OpenScape Business auch über das Internet erreichbar sein. Für

alle Beispiele in diesem Kapitel wird das folgende grundlegende Netzwerkszenario angenommen.



Beschreibung des Netzwerkszenarios

OpenScape Business befindet sich in der Büroumgebung, die über den Bürorouter mit dem Internet verbunden ist. Dieser Router ist vom Internet aus entweder über die öffentliche IP-Adresse "62.38.100.120" oder über einen DNS-Namen erreichbar.

Der myPortal @work-Client ist mit dem LAN innerhalb eines Heim- oder externen Netzwerks verbunden, das über einen separaten Router mit dem Internet verbunden ist. Der externe Router ist aus dem Internet mit der öffentlichen IP-Adresse "82.69.132.24" erreichbar.

Konfigurationsschritte

Um den myPortal @work-Client auf dem OpenScape Business über das Internet nutzen zu können, müssen die folgenden Komponenten entsprechend konfiguriert werden.

OpenScape Business im Büro

Aktive STUN-Unterstützung auf dem System, falls nicht bereits für einen ITSP geschehen.

Konfigurieren Sie den myPortal @work-Benutzer (SBC-Flag ist für VoIP nicht erforderlich)

Büro-Router

Damit der myPortal @work-Client OpenScape Business vom Internet aus erreichen kann und umgekehrt, muss die folgende Konfiguration auf dem Router im Büro vorgenommen werden:

- HTTPS-Port-Weiterleitung vom externen Port (Standard ist 8802) auf den internen Port 8802 des Systems
 - Externer Port (Standard ist 8802) -> Büro-Router -> 192.168.1.30:8802

myPortal @work / externer Router

Der myPortal @work-Client muss sich mit der öffentlichen IP-Adresse oder dem DNS des Internet-Routers im Büro auf dem externen Port verbinden, der standardmäßig 8802 ist (aufgrund der zuvor konfigurierten Port-Weiterleitung zeigt dieser auf OpenScape Business im Büronetzwerk).

In den meisten Fällen muss auf dem externen Router nichts zusätzlich konfiguriert werden.

11.2.1.4 Weitere Konfigurationshinweise & Einstellungen

Einstellungen des STUN-Servers

Weitere Informationen zur Konfiguration des STUN-Servers finden Sie im Kapitel "STUN konfigurieren" in der Anleitung "[So konfigurieren Sie das Systemgerät@home](#)" und im OpenScape Business V3, my Portal @work, Benutzerhandbuch im Abschnitt "So fügen Sie einen STUN-Server hinzu".

Headsets

Jedes erkannte Audiogerät/Mikrofon des Betriebssystems kann verwendet werden.

Integration von Jabra/Plantronics-Headsets

Führen Sie bei Problemen mit der Integration von Jabra-Headsets die Anwendung mit Administratorrechten aus.

Um die Jabra-Headset-Integration nutzen zu können, muss das Jabra-Gerät in myPortal @work als Hauptmikrofon eingestellt werden.

Für die Integration von Plantronics muss der Plantronics-Hub installiert sein.

Ports und Firewall-Einstellungen

Grundsätzlich müssen die folgenden Ports für die Signalisierung von myPortal @work konfiguriert werden:

- UC-Funktionalität und WebRTC/VoIP-Signalisierung: 8802
- Standard-Port des STUN-Servers: 3478. Wenn ein benutzerdefinierter STUN-Server konfiguriert ist, ist möglicherweise ein anderer Port erforderlich.

Die Konfiguration der Ports für WebRTC/VoIP-Nutzdaten hängt von der Art der in der Kundenumgebung verwendeten Firewall ab. Um myPortal @work in einer Kundennetzwerkumgebung zu betreiben, muss unbedingt der Typ der verwendeten Firewall erfasst und überprüft werden, ob sie zustandsbehaftet oder zustandslos ist, und die Firewall-Einstellungen müssen zusammen mit dem zuständigen IT-Administrator konfiguriert werden.

Zum besseren Verständnis der Unterschiede zwischen den beiden Arten von Firewalls lesen Sie bitte die folgenden Ausführungen:

- Zustandslose Firewalls sind so konzipiert, dass sie Netze auf der Grundlage statischer Informationen wie Quelle und Ziel schützen.
- Bei einer zustandsbehafteten Firewall wird der vollständige Status aktiver Netzwerkverbindungen überwacht. Das bedeutet, dass zustandsbehaftete Firewalls ständig den gesamten Kontext des Datenverkehrs und der Datenpakete analysieren.

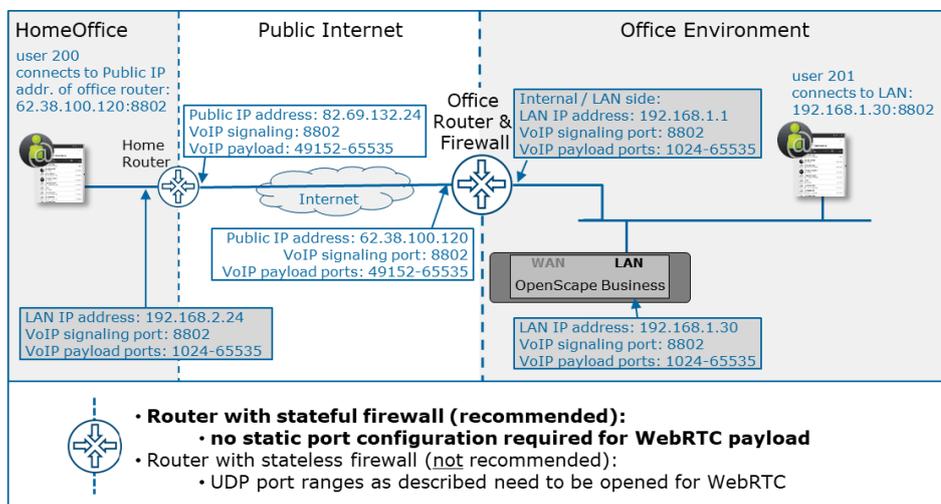
Weitere Informationen zu diesen Firewall-Typen finden Sie im Internet oder in einschlägiger Fachliteratur.

Atos Unify geht davon aus, dass ein NAT-Gerät mit zustandsbehafteter Firewall verwendet wird, um private Kundennetze besser zu schützen. Das bedeutet, dass dieses Gerät interne ausgehende Verbindungen zu ihrem Ziel zulassen muss.

Die Firewall bzw. das NAT-Gerät blockiert alle Pakete in eingehender Richtung, es sei denn, sie gehören zu einer bereits aufgebauten Sitzung (an einem ephemeren/dynamischen Port), die zuvor in ausgehender Richtung aufgebaut wurde.

In Bezug auf die Portnutzung muss in der Firewall/dem NAT-Gerät nichts konfiguriert werden, da dies bei Verwendung einer zustandsbehafteten Firewall automatisch erfolgt und abgewickelt wird.

Zur Ausführung sicherer WebRTC-basierter VoIP-Lösungen ist eine zustandsbehaftete Firewall zu empfehlen.



Im Rahmen einer zustandslosen Firewall (die für VoIP nicht empfohlen wird) muss der folgende Bereich von UDP-Quellports für Geräte innerhalb des Kundennetzes für den internen Nutzdatenverkehr geöffnet werden: 1024-65535.

Für den gesamten Nutzdatenverkehr, der über das Internet ausgetauscht wird, verwendet die WebRTC-Technologie Ports aus dem UDP-Portbereich von 49152-65535. Für weitere Informationen verweisen wir auf einschlägige Fachliteratur als Informationsquelle.

Jedes Netzwerkgerät auf dem Pfad zwischen den beteiligten Nutzdatenendpunkten muss entsprechend konfiguriert werden (z. B. Router, Firewall, NAT, Proxy usw.).

Aufgrund des breiten Portbereichs, der geöffnet werden muss, ist eine zustandslose Firewall für VoIP nicht zu empfehlen.

Tabelle 4:

	Zustandsbehaftete Firewall	Zustandslose Firewall, die statisch geöffnet wird
WebRTC-/VoIP-Signalisierungsport	8802	8802
WebRTC/VoIP-Nutzdaten UDP-Portbereich im lokalen LAN, d. h. in der Kundenumgebung	dynamisch ⁴	1024-65535
WebRTC/VoIP-Nutzdaten Über das öffentliche Internet verwendeter UDP-Portbereich	dynamisch ⁴	49152-65535

Einschränkungen für VoIP

- In Szenarien mit mehreren Anrufen (z. B. Vermittlung, Konferenz, Anklopfen) empfehlen wir, die Headset-Integration im Fehlerfall zu deaktivieren. Durch die Deaktivierung der Headset-Integration in myPortal @work kann nur die Verbindungssteuerungsfunktion des Headsets nicht genutzt werden, das Headset kann aber weiterhin als Audiogerät verwendet werden.
- Die Funktion "Freie Platzwahl" von myAgent (der Agent kann das zu verwendende Telefon während des Anmeldevorgangs über ein Dropdown-Menü auswählen), d. h. die freie Auswahl eines physischen Geräts durch einen Agenten, wird in Kombination mit myPortal @work nicht unterstützt.
- Die symmetrische NAT-Konfiguration wird nicht unterstützt.
- Strenge Firewalls werden nicht unterstützt.

11.2.1.5 Leitfaden zur Fehlerbehebung**Zeitüberschreitung der Verbindung**

- Als Heimanwender mit VPN-Verbindung sollten Sie sicherstellen, dass der Anwender auf die LAN-Adresse des Systems zugreifen und sich mit der LAN-Adresse: 8802-Port verbinden kann. Meldung zur Fehlerbehebung: Fehlermeldung "Time-out der Verbindung", Aktion: Prüfen Sie, ob der Benutzer bei der Verbindung über VPN eine lokale IP aus dem VPN-Netzwerk hat.
- Stellen Sie als Einzelbenutzer sicher, dass kein anderes Gerät und kein VoIP myPortal @work-Client mit derselben Rufnummer

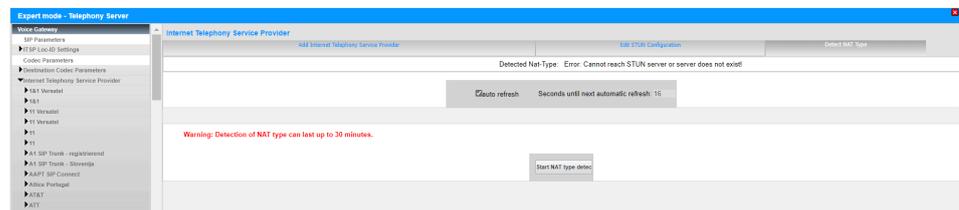
⁴ Keine Konfiguration erforderlich; die Ports werden dynamisch aus demselben UDP-Portbereich wie bei der zustandslosen Firewall genommen

registriert ist. Prüfen Sie auch unter **WBM > Expertenmodus > Web Services Assistant** die offenen Verbindungen.

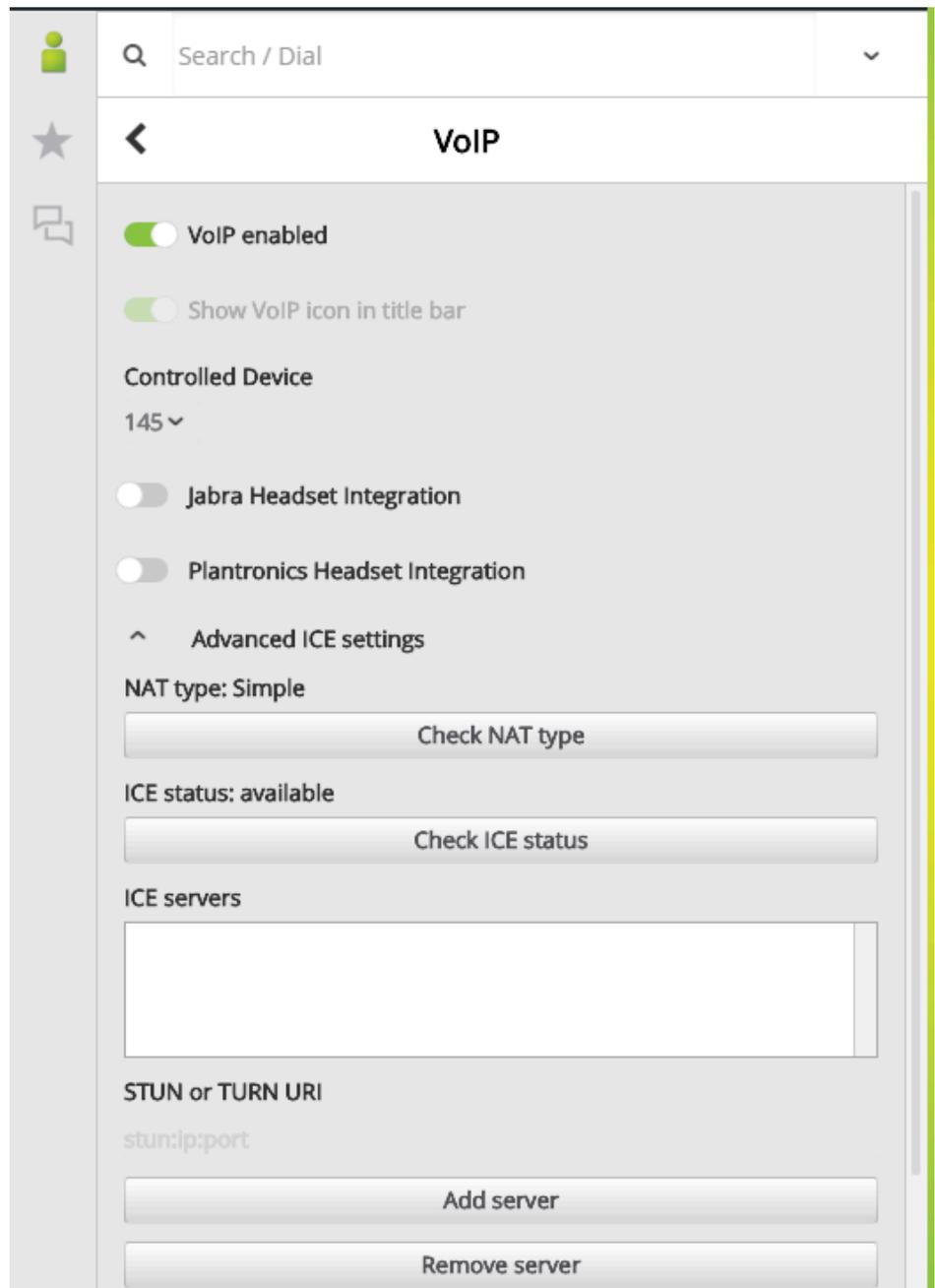
Keine Nutzdaten

Falls dauerhaft keine Nutzdaten ausgegeben werden:

- Vergewissern Sie sich, dass die zulässigen Ports an der Firewall geöffnet sind.
- Überprüfen Sie die NAT-Firewall-Konfiguration. Die symmetrische NAT-Konfiguration wird nicht unterstützt.
- Sie können den NAT-Typ vom System aus unter **WBM > Expertenmodus > Sprachgateway > NAT-Typ erkennen** ermitteln.
- Überprüfen Sie die Anbindung des STUN-Servers im System.



- Prüfen Sie die ICE-Anbindung in myPortal @work: **Einstellungen > VoIP > Erweiterte ICE-Einstellungen**. Falls "NAT-Typ" und/oder "ICE-Status" nicht wie unten dargestellt sind, müssen die Netzwerk-/Firewall-Einstellungen von Ihrem Administrator überprüft werden.



Führen Sie "NAT-Typ prüfen" > NAT-Typ aus: Einfach

Führen Sie "ICE-Status prüfen" > ICE-Status aus: verfügbar

- Deaktivieren Sie die Headset-Integration in myPortal @work und führen Sie das Szenario erneut durch.
- Wählen Sie in den VoIP-Einstellungen erneut Audiogeräte aus.

11.2.1.6 Weitere Hinweise

SIP ALG (Application Layer Gateway – Gateway auf Anwendungsebene)

Wenn eines der folgenden Probleme auftritt, überprüfen Sie bitte, ob ein SIP ALG auf einem der beteiligten Router aktiviert ist. Es gibt verschiedene Kategorien von Symptomen, die das SIP ALG bei VoIP-Verbindungen hervorrufen kann. Das ist nicht immer offensichtlich, zumal diese Probleme oft unbemerkt von den Benutzern auftreten.

- Einweg-Audio (nur eine Person kann die andere hören)
- Der Client klingelt nicht, wenn er angerufen wird
- Anrufe werden nach dem Verbinden abgebrochen
- Anrufe, die ohne erkennbaren Grund direkt zur Voicemail umgeleitet werden

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).
E-Mail-Adresse	E-Mail-Adresse des Teilnehmers.

Einstellungen	Erklärung
Voicemail an E-Mail	Aktivierung/Deaktivierung der Email-Benachrichtigung beim Eingang einer neuen Sprachnachricht.
Sichtbarkeit des Anwesenheitsstatus	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	

11.4 Anwesenheitsstatus (Präsenz)

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 @work oder myPortal to go ändern. Bei jeder Änderung des Anwesenheitsstatus außer für **Büro** können Sie bei Bedarf 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**

Anmerkung: Der Systemadministrator kann die Sichtbarkeit des Status „krank“ innerhalb der Systemadministration ein- und ausschalten. Siehe [OpenScape Business UC Suite > Server](#)

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.

11.5 Verzeichnisse und Journal

Verzeichnisse und das Journal organisieren Kontakte und Anrufe.

11.5.1 Verzeichnisse

Verzeichnisse organisieren die Kontakte der Teilnehmer. Teilnehmer können mit UC Smart Clients auf Kontakte zugreifen.

Das System stellt folgende Verzeichnisse mit den folgenden Funktionen und folgender Prioritätsreihenfolge für die Rufnummernsuche bereit (Nummernsuche wird nur für externe Anrufe unterstützt, und für den Fall, dass Amt bzw. ITSP den Namen nicht bereitstellen):

Verzeichnis	UC Smart Clients	Systemtelefon mit Display
Persönliches Verzeichnis	Über den persönlichen Assistent 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. Interne Teilnehmer mit Systemtelefon werden mit Anwesenheitsstatus dargestellt. Voraussetzung für die Anzeige des Anwesenheitsstatus eines Teilnehmers ist, dass der betreffende Teilnehmer dies zulässt.	
Systemverzeichnis	Enthält alle zentralen Kurzwahlnummern.	

Anmerkung: Geben Sie Rufnummern in Verzeichnissen nach Möglichkeit stets im kanonischen Format ein.

11.5.2 Internes Verzeichnis

Das interne Verzeichnis enthält die Kontaktdetails der internen Teilnehmer und der MULAP-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.

Ob interne Teilnehmer und Gruppen im internen Verzeichnis angezeigt werden, ist abhängig von dem Teilnehmer-Parameter **Eintrag im Telefonbuch** (einstellbar im WBM über die Teilnehmer-Wizards).

Im Netzwerk gilt das interne Verzeichnis knotenübergreifend.

Zugehörige Konzepte

[Gruppenruf](#) auf Seite 372

11.5.3 Favoritenliste

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 der Rufzustand des Teilnehmers angezeigt. Der UC Smart Benutzer kann diesen Anruf übernehmen. Zusätzlich wird der Anwesenheitsstatus für interne Teilnehmer angezeigt.

11.5.4 Systemverzeichnis

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 Unified-Verzeichnis

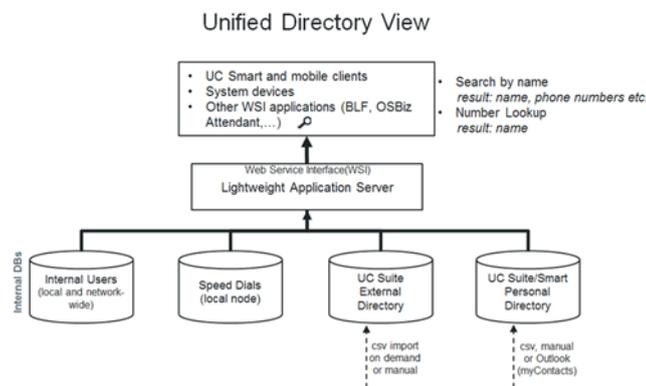
OpenScape Business bietet verschiedene Datenquellen zum Speichern und Abrufen von Teilnehmer- oder Kontaktdaten – von internen Teilnehmerdaten in der internen Benutzerkonfiguration über die interne Kurzwahlliste bis hin zu den verschiedenen Verzeichnissen der UC-Anwendungen.

Jede Datenquelle in OpenScape Business wird von einer bestimmten Client-Anwendung verwendet, die entweder Teil der Systemsoftware auf den Telefongeräten oder Teil einer UC-Client-Anwendung ist.

Abhängig von den verwendeten Datenquellen und Clients werden die Daten unterschiedlich abgerufen und dargestellt.

Der Unified-Verzeichnisdienst in OpenScape Business nutzt die bestehenden OpenScape Business-Datenquellen für die Funktionen Rufnummernsuche und Namensauflösung. Er übermittelt an alle Systemgeräte und OpenScape Business-Clients einheitliche Suchergebnisse und Namensauflösungsinformationen.

Der Zugriff auf den Unified-Verzeichnisdienst kann entweder über das Web Service Interface (WSI) mit externen Clients wie myPortal to go oder intern über Anrufbearbeitungsmechanismen (z. B. von OpenStage-Telefonen) erfolgen.



Der Unified-Verzeichnisdienst verwendet die folgenden internen Datenbanken und Verzeichnisse von OpenScape Business:

- Internes Benutzerverzeichnis (netzweit)
- Kurzwahllisten
- UC Smart Persönliches Verzeichnis (optional)
- UC Suite Externes Verzeichnis (optional)
- Persönliche Outlook-Kontakte (falls importiert über myContacts)

Der Unified-Verzeichnisdienst ist auf allen Knoten eines OpenScape Business-Systems ab V2R2 verfügbar. Es erfordert keine spezielle Hardware, Software oder zusätzliche Lizenzen.

Um bei der Verwendung des Unified-Verzeichnisdienstes die besten Ergebnisse zu erzielen, sollten Sie einige Regeln für Rufnummernformate und zur Schreibweise von Namen beachten.

11.5.5.1 Leistungsmerkmale

Unterstützte Geräte/Clients

Der Unified-Verzeichnisdienst stellt folgende Funktionen bereit:

- Telefonbuchsuche in mehreren internen Datenquellen von OpenScape Business
- Einheitliche Bereitstellung des Suchergebnisses für alle unterstützten Kunden
- Rufnummernsuche / Namensauflösung in mehreren internen Datenquellen

- Einheitliche Bereitstellung der Namensauflösungsergebnisse für alle unterstützten Clients
- Externer Datenzugriff über die WebServices-Schnittstelle (WSI)

Die Leistungsmerkmale sind für Einzelknotensysteme wie folgt verfügbar. In OpenScape Business-Netzwerken hängt die Verfügbarkeit der Features hauptsächlich von der Art der Verbindung der Amtsleitungen, Geräte und Clients innerhalb des Netzwerks ab.

Unified Directory unterstützt folgende Clients/Systemgeräte von Unify unter Verwendung der angegebenen Schnittstellen:

Gerät/Client	Verwendete(s) Schnittstelle/Protokoll	Hinweise
OpenStage-Telefone	Anrufverarbeitung/ HFA-Protokoll	WSI/HTTP(S) ist optional für OpenStage 60/80 für Anrufer-Bilder
OpenScape DeskPhone IP	Anrufverarbeitung/ HFA-Protokoll	WSI/HTTP(S) ist optional für DeskPhone IP 55 für Anrufer-Bilder
Schnurlose (CMI)- Geräte	Anrufverarbeitung/ CMI-Protokoll	
CP 100/110/200/210	Anrufverarbeitung/ HFA-Protokoll	
DeskPhone CP400/ 600/600E/ 700/700X/710	WSI/HTTP(S)	
myPortal @work	WSI/HTTP(S)	
myPortal to go	WSI/HTTPS	
OpenScape Business Attendant/BLF	Anrufverarbeitung/ CorNet-Protokoll	WSI/HTTP(S) ist optional

Anmerkung: Die UC Suite myPortal-, myAttendant- und myAgent-Clients verwenden eigene Mechanismen für die Verzeichnissuche und Namensauflösung.

Suchfunktion

Die Unified Directory-Suche wird immer unter Verwendung der spezifischen Geräte-/Client-Benutzerschnittstelle durchgeführt. Die Suchkriterien und der verwendete Zeichensatz können abhängig von den verwendeten Clients eingeschränkt sein.

Nach Eingabe des Suchkriteriums wird die Suche in den nachfolgenden Verzeichnissen durchgeführt

- Internes Benutzerverzeichnis (netzwerkweit)
- Kurzwahllisten
- UC Smart Persönliches Verzeichnis (optional)
- UC Suite Externes Verzeichnis (optional)

- Persönliche Outlook-Kontakte (falls über myContacts importiert)

Alle Übereinstimmungen innerhalb der obigen Verzeichnisse werden zusammen mit ihrer Herkunft als Suchergebnisse angezeigt. Die Übereinstimmungen enthalten entweder den vollständigen Kontaktdatenatz oder nur Teile davon. Die Informationstiefe der Ergebnisse hängt von der Datenquelle ab.

Anmerkung: Die Suche nach Gruppennamen in myPortal @work wird im UC Suite-Modus nicht unterstützt. Es wird nur die Suche nach lizenzierten Benutzern (Basislizenz) und lizenzierten MULAP-Gruppen (UC-Einträge) unterstützt.

Die Übereinstimmungen werden auf den Geräten oder Clients angezeigt, abhängig von den Anzeigefähigkeiten.

	Internes Benutzerv	Kurzwahl	UC Smart Persönlich Verzeichn	UC Suite Externes Verzeichn	Persönliche Outlook-Kontakte (über myContacts)
Nachname	X	---	X	X	X
Vorname	X	---	X	X	X
Kurz-/Anzeigename	X	X	---	---	---
Büro-Rufnr.	---	---	X	X	X
Private/ext. Rufnr.	---	---	X	---	X
Mobilrufnr.	---	---	X	X	X
E-Mail-Adr.	---	---	X	X	X
Firmenname	--	---	X	X	X
Ort	---	---	---	---	---
Kontaktbild	---	---	X	---	X
Kontaktbildvorschau	---	---	X	---	X

Rufnummernsuche

Mit der einheitlichen Rufnummernsuche wird der Anrufer (CLI) durch eine Nummernsuche in allen unterstützten internen Datenquellen aufgelöst. Die Suche wird in den folgenden Rufnummer-Feldern durchgeführt:

- Büro-Rufnummer
- Mobilrufnummer
- Private Rufnummer

Die Rufnummernsuche wird im Allgemeinen bei eingehenden oder ausgehenden Anrufen ausgelöst, wobei bestimmte Routing- und Weiterleitungsfunktionen zusätzlich berücksichtigt werden.

Eine feste Priorisierung der Datenquellen, die für die Rufnummernsuche verwendet werden, wird implementiert, um so schnell wie möglich ein Ergebnis zu erhalten. Das Ergebnis enthält entweder nur den Nachnamen, den Vornamen, den Anzeigenamen oder, sofern verfügbar, die vollständigen Kontaktdaten.

Tabelle 5: Unterstützte Datenquellen und Priorisierung

Priorität	Datenquellen	Bemerkung
1	CO ITSP Name (wie vom Provider gesendet)	Voraussetzung ist, dass das Flag "Name im Amt" aktiviert wird.
2	Kurzwahlliste	
3	Persönliche Kontakte	
4	UC-Benutzerdetails	

Die abgerufenen Daten werden auf dem Gerät des Benutzers und/oder im UC-Client angezeigt. Die Informationstiefe der Ergebnisse hängt von den Anzeigefähigkeiten ab.

• **Kommende Rufe**

Unterstütztes Szenario für Einzelknotensysteme:

- Basic Call
- Gruppenruf/MULAP-Ruf
- Rufzuschaltung
- Einzelschritt-Übergabe (SSCT)
- Gespräch übergeben/Übergabe nach Melden/Rückfrage
- Uneingeschränkte Gesprächsumleitung (CFU)
- Verzögerte Anrufumleitung (CFNR = Call Forwarding No Reply)
- Anrufumleitung bei Besetzt (CFB = Call Forwarding Busy)
- Übergabe ohne Rückfrage
- Anrufübernahme

Anmerkung: Anrufübernahme unterscheidet sich von Anrufübernahmegruppe. Wenn in der Anrufübernahmegruppe eine externe Nummer im Unified Directory gespeichert ist, wird der Name des Anrufers von den Mitgliedern der Gruppe nicht angezeigt.

Unterstütztes Szenario für mehrere Knoten (Netzwerk). Szenario ist ein Gateway-Anruf.

• **Gehender Anruf**

Im Falle eines ausgehenden Anrufs erfolgt die Rufnummernsuche für die gewählte Teilnehmernummer nur einmal.

Unterstütztes Szenario für Einzelknotensysteme ist ein Basic Call an eine externe Rufnummer.

Die Darstellung der Rufnummer-Suchergebnisse hängt von den Anzeigefähigkeiten der Telefone ab.

11.5.5.2 Regeln und Konventionen

Bei den Rufnummern- und Namensformaten innerhalb der Datenquellen sind einige Konventionen zu beachten, um optimale Ergebnisse mit dem Unified-Verzeichnisdienst zu erhalten.

Unterstütztes Rufnummernformat

Alle externen Rufnummern innerhalb der Datenquellen müssen einschließlich Länder- und Ortsvorwahl im kanonischen Format eingegeben werden, z. B. +4989700712345

Die Kurzwahlliste unterstützt nur das vom System wählbare Format (z.B. 0089700712345 oder 0004989700712345)

Wenn Kurzwahlnummern so konfiguriert sind, dass sie über LDAP zugänglich sind, müssen Sie die Option zur Nummernkonvertierung aktivieren, um den Kontaktnamen anzuzeigen, wenn die Nummer im kanonischen Format vorliegt. Weitere Informationen zum Aktivieren der Nummernkonvertierung finden Sie unter [Wie Sie eine externe Datenquelle für Open Directory Service hinzufügen](#).

Unterstützte Namensformate

Bei Namensformaten und Zeichensätzen sind die folgenden Konventionen zu beachten:

- **Namensformat bei Kurzwahl**

Die Namenssuche innerhalb der Kurzwahlliste wird nur in Kombination mit bestimmten Konfigurationsregeln unterstützt. Vor- und Nachname müssen im vorhandenen Namensfeld nach dem folgenden Muster eingegeben werden:

<Nachname>, <Vorname> (kommagetrennt)

- **Interne Teilnehmer bei Migrationsszenarien**

Bei internen Teilnehmern, die diese Konfigurationsregeln nicht beachten, wird eine Migration auf V2R1 und höher ggf. unerwartete Folgen und wird nicht ordnungsgemäß unterstützt. Dies bedeutet, dass der Administrator interne Namen vor Durchführung der Migration in das folgende Format konvertieren sollte:

<Nachname>, <Vorname> (kommagetrennt)

Verfügbarkeit von Verzeichnisänderungen

Nach dem Erstellen, Aktualisieren oder Löschen von Kontakten in den verschiedenen Datenquellen kann es bis zu 10 Minuten dauern, bevor alle Änderungen in den Suchergebnissen sichtbar sind.

11.5.5.3 Funktionale Grenzen

Für Unified-Verzeichnisse gelten die folgenden funktionalen Grenzen:

Namenssuche

- Unterstützung von Gruppennamen

Gruppennamen (nicht MULAP-Namen) können zurzeit nicht in allen Arten von Konfigurationen durchsucht werden

- Unterstützung von Sonderzeichen

Auf den meisten Telefongeräten kann der Benutzer nur nach den Standardzeichen "a-z" suchen. Die Eingabe von (diakritischen) Sonderzeichen (wie z.B. der deutschen Umlaute Ää, Öö, Üü oder ß) ist über die Benutzeroberfläche des Telefongeräts nicht möglich.

Daher beinhaltet ein Suchergebnis mit einfachen Zeichen auch Sonderzeichen. Bei einer Suche mit den Zeichen „acdegilnorstuyz“ sind auch die entsprechenden Sonderzeichen "àáâãäå#äçćčďđèéêëëë#ìíîíłńñňòóôõöőřśšţùúûüýÿžžž" im Suchergebnis enthalten.

Anmerkung: Eine Suche im Telefonbuch mit Platzhalterzeichen am Anfang des Suchbegriffs, z. B. <*jo*>, wird nur für interne Benutzer unterstützt.

- Unterstützung von Kurzwahlnamen

Die Namenssuche innerhalb der Kurzwahlliste wird nur in Kombination mit bestimmten Konfigurationsregeln unterstützt. Vor- und Nachname müssen im vorhandenen Namensfeld nach einem der folgenden Muster eingegeben werden

- <Nachname>, <Vorname> (kommagetrennt)
- <Nachname>, <Vorname> (Leerschritt als Trennzeichen)

Namensanzeige

Persönliche Kontakte aus UC Smart und dem externen Offline-Verzeichnis, bei denen Vorname und Nachname zusammen länger als 24 Zeichen sind, werden zwecks Anzeige auf dem Gerätedisplay auf 24 Zeichen gekürzt.

Rufnummernsuche

Die Funktion Rufnummernsuche (Kontaktname aus Rufnummer des Anrufers ermitteln) wird vom Unified-Verzeichnisdienst für SIP- und S0-Geräte nicht unterstützt.

11.5.5.4 Unified-Verzeichnis in vernetzten Systemen

Der Unified-Verzeichnisdienst ist auf allen Knoten eines OpenScape Business-Netzwerks aktiv und nutzt die Datenquellen des eigenen Systems. Telefongeräte und Clients verwenden innerhalb ihres eigenen Knotens immer den Unified-Verzeichnisdienst.

Es kommt daher auf die Art des Datenquelleninhalts an, ob netzweite Kontakte verfügbar sind oder nicht.

Tabelle 6: Lokale und netzweite Datenquellen

Datenquelle	Lokale Daten	Netzweite Daten
Internes Benutzerverzeichnis	X	X
Kurzwahllisten	X	---
UC Smart Persönliches Verzeichnis	X	---
UC Smart Persönliches Verzeichnis	X	---
Persönliche Outlook-Kontakte (über myContacts)	X	---

Rufnummernsuche

In Vernetzungsszenarien wird die Funktion Telefonnummer suchen nicht verwendet. In solchen Fällen wird der Name über normale Vernetzungsmechanismen zwischen den Netzknoten übertragen.

Für interne Teilnehmer wird der konfigurierte Anzeigename verwendet, so dass eine Suche nicht erforderlich ist.

11.5.6 Journal

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.

Dem UC Smart Benutzer werden max. die letzten 100 Anrufe angezeigt.

Ordner für Anrufarten

Die Anrufe können in folgende Gruppen gegliedert sein:

- **Offen**
- **Entgangen**
- **Angenommen**
- **Alle Anrufe**

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 die **Richtung**

des Anrufs und **Dauer** sowie ggf. erfolgte Weiterleitungen oder Anrufübernahmen.

11.6 Anrufe

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 Landeskenzahl, Ortskenzahl 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.	<ul style="list-style-type: none"> • 321 (intern) • 0700798765 (eigenes Ortsnetz) • 0089700798765 (fremdes Ortsnetz) • 0004989700798765 (Ausland)

Tipp: Verwenden Sie wo immer möglich das kanonische Rufnummernformat. Damit ist eine Rufnummer in jeder Situation vollständig und eindeutig und für Vernetzung und mobile Teilnehmer konsistent.

Bei der manuellen Wahl (wählbares Format) einer externen Rufnummer muss die Amtskennzahl immer mitgewählt 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).

Anmerkung: Bei Anrufen innerhalb der USA über CSTA zu einer Rufnummer im kanonischen Format wird die Rufnummer in das wählbare Format konvertiert.

11.6.2 Voraussetzungen für den Empfang von VoIP-Anrufen auf myPortal to go mit CallKit auf Ihrem iPhone

Die VoIP-Anrufbenachrichtigungen von iOS basieren auf dem APNS-Mechanismus von Apple.

Dieser Dienst erfordert Folgendes:

- Einen konfigurierten DNS-Server, der öffentliche Domännennamen aus dem Internet auflöst.
- Internetzugang für OpenScape Business System (Port TCP/443 ausgehend), um APNS-Anrufbenachrichtigungen zu senden.
- Die Systemsoftware muss auf dem neuesten Stand der Haupt-, Neben- und Korrekturversionen sein. Die neueste Systemversion ist wichtig, da der APNS-Dienst bestimmte Zertifikate benötigt, die bei älterer Systemsoftware ablaufen.

11.7 Konferenzen

In einer Konferenz können mehrere Teilnehmer (darunter auch externe) gleichzeitig miteinander telefonieren. Mit der Konferenz-Management-Funktion können Sie Konferenzen schnell und einfach durchführen und im Voraus planen.

Telefon- und applikationsgesteuerte Konferenzen

Als Teilnehmer können Sie Konferenzen sowohl über das Telefon einleiten als auch über die Applikationen von UC Smart.

Eine telefongesteuerte Konferenz können Sie auf folgende Arten starten und anschließend am Telefon steuern:

- Gewünschte Konferenzteilnehmer anrufen und mit der Konferenz verbinden
- Rückfragegespräch zu einer Konferenz erweitern
- Zweitanruf zu einer Konferenz erweitern

Applikationsgesteuerte Konferenzen können Sie über das Konferenz-Management einleiten, steuern und verwalten. Für die Nutzung des Konferenz-Managements ist eine Konferenz-Lizenz erforderlich.

Unterschiede zwischen den Konferenzarten:

	Telefongesteuerte Konferenz	Applikationsgesteuerte Konferenz
Richtung des Verbindungsaufbaus aus Sicht des Systems	<ul style="list-style-type: none"> • Gehend 	<ul style="list-style-type: none"> • Ankommend (Einwahl durch den Teilnehmer)
Authentifizierung der Konferenzteilnehmer	-	<ul style="list-style-type: none"> • Persönliche PIN (Konferenz-ID) • Gast PIN (optional)

	Telefongesteuerte Konferenz	Applikationsgesteuerte Konferenz
Vordefinierte Einladung an die Konferenzteilnehmer	-	<ul style="list-style-type: none"> • Name der Konferenz • Einwahlnummer (MeetMe) • Persönliche PIN (Konferenz-ID) • Gast PIN (optional)
Max. Anzahl der Teilnehmer pro Konferenz	8	16

Geplante Konferenz

Geplante Konferenzen werden als permanente Konferenzen angelegt. Die Konferenz kann ohne weitere Terminplanung bei Bedarf jederzeit genutzt werden. Geplante Konferenzen belegen keine Konferenz-Channels, solange sich keine Teilnehmer in der Konferenz eingewählt haben. Die Reihenfolge der Einwahl bestimmt über die Belegung der Konferenz-Channels.

Administratoren können bei der Ersteinrichtung über das WBM die festgelegte Einwahlnummer (MeetMe) für Konferenzen ändern. Den Teilnehmern wird die Einwahlnummer angezeigt, mittels derer sie sich in die Konferenz einwählen können. Dabei müssen sie sich mit ihrer persönlichen PIN oder falls zugelassen mit der allgemeinen Gast-PIN authentifizieren.

Moderatoren

Der Initiator einer Konferenz ist automatisch Moderator und hat folgende Möglichkeiten:

- Geplante Konferenzen anlegen, bearbeiten und löschen.
- Konferenzteilnehmer hinzufügen und entfernen.
Entfernte Teilnehmer bleiben nicht in der Konferenz.
- Konferenzteilnehmer trennen.
Getrennte Teilnehmer können sich erneut in die Konferenz einwählen.
- Einen anderen internen Teilnehmer desselben Knotens als Moderator festlegen.
- Die Konferenz verlassen, ohne sie sofort zu beenden.
Verlässt der letzte Moderator die Konferenz, endet sie nach 5 Minuten.
- Aktive Konferenzen beenden.
- In einer aktiven Konferenz eine Web Collaboration-Sitzung starten.
- Vordefinierte Einladungen an alle oder einzelne Konferenzteilnehmer verschicken.

Alle internen Teilnehmer innerhalb eines Knotens können Moderatoren werden. Dafür ist allerdings eine Konferenz-Lizenz erforderlich.

Konferenzteilnehmer, deren Kontaktdaten manuell eingegeben wurden, werden als externe Teilnehmer behandelt und können nicht als Moderatoren festgelegt werden.

Konferenzteilnehmer

Konferenzteilnehmer können die Konferenz verlassen und sich erneut einwählen. Zusätzlich können sie an einer bereits gestarteten Web Collaboration-Sitzung teilnehmen. Solange eine Konferenz nur einen Teilnehmer hat, hört dieser Wartemusik. Die maximale Anzahl der externen Konferenzteilnehmer ist unter anderem durch die Anzahl der verfügbaren Amtsleitungen begrenzt.

Automatisches Beenden ohne Moderator

Verlässt der letzte Moderator die Konferenz, werden die Teilnehmer mit einem Hinweistext informiert, dass die Konferenz ca. in 5 Minuten endet.

Benachrichtigung der Konferenzteilnehmer

Der Moderator kann allen oder einzelnen Konferenzteilnehmern eine Einladung per E-Mail zuschicken. Voraussetzung ist, dass auf dem Client-PC ein E-Mail-Programm installiert ist. Bekannte E-Mail-Adressen werden automatisch in den Verteiler eingefügt. Bei einer Einladung an alle Konferenzteilnehmer wird nur die allgemeine Gast-PIN (falls zugelassen) verschickt, bei individuellen Einladungen wird zusätzlich die persönliche PIN verschickt.

Alternativ kann ein vordefinierter Einladungstext zur Weiterverwendung in anderen Programmen (z. B. Chat) in die Zwischenablage kopiert werden.

11.8 Web Collaboration

myPortal unterstützt innerhalb von Telefongesprächen und Konferenzen die Einbindung des separaten Produktes Web Collaboration für die gleichzeitige multimediale Zusammenarbeit. Diese bietet schnellen Zugriff auf Funktionen wie Desktop- und Anwendungsfreigabe, Dateifreigabe, Co-Browsing, Whiteboarding, URL-Push, IM-Chat und Video-Chat mit mehreren Teilnehmern.

Die Web Collaboration kann von einem Teilnehmer während eines Telefongesprächs über das Anruf-Fenster des UC PC-Clients oder innerhalb einer aktiven Konferenz vom Moderator gestartet werden. Es öffnet sich eine Webseite, über die der Download des Web Collaboration-Clients eingeleitet werden kann. Eine lokale Installation von Web Collaboration auf dem UC PC-Client ist nicht erforderlich. Ist auf dem UC PC-Client ein E-Mail-Programm hinterlegt, kann den Gesprächsteilnehmern eine E-Mail mit dem Link auf den Web Collaboration-Client zugesendet werden. Detaillierte Informationen zur Web Collaboration finden Sie in der Web Collaboration-Produktdokumentation.

Beim Löschen oder Beenden einer Konferenz wird die zugehörige Web Collaboration-Sitzung automatisch gelöscht.

Einbindung von Web Collaboration

Für die Einbindung von Web Collaboration muss der Administrator im WBM die Lizenznummer und das Passwort für die gehostete Web

Collaboration-Verbindung eingeben. Der Hersteller bietet den Web Collaboration-Server im Internet als Dienst an (Öffentlicher Server). Über eine gesicherte https-Verbindung werden Lizenznummer und Passwort übertragen. Standardmäßig wird dafür der TCP-Port 5100 verwendet. Lokale Web Collaboration-Server werden nicht unterstützt.

Anmerkung: Für die Nutzung von Web Collaboration benötigen die UC PC-Clients und das Kommunikationssystem eine Internetverbindung. Verbindungen über Proxy werden vom Kommunikationssystem nicht unterstützt.

Instant Messaging und Web Collaboration

Instant Messaging des Systems und Instant Messaging von Web Collaboration sind voneinander unabhängig: Sofortnachrichten aus einem UC PC Client erscheinen nicht in einer Web Collaboration Sitzung desselben Teilnehmers und umgekehrt.

11.9 Instant Messaging

Instant Messaging ist die Kommunikation mittels Sofortnachrichten (Chat).

11.9.1 Instant Messaging

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 begrenzte Zahl von Sofortnachrichten. Es werden max. die letzten 100 Sofortnachrichten eines Benutzers angezeigt.

11.10 Sprachbox (SmartVM)

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 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-Sprachbox wird vom Teilnehmer über das Telefon oder über den UC Smart Client 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** (vergleichbar mit Xpressions Compact/EVM)
 - Telefonmenü, UC Suite: **OSO** (vergleichbar mit 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

Anmerkung: 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 vorgelegte 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. absteigenden 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 S₀-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.

Anmerkung: Für die Voicemail-Wiedergabe über externe Rufnummern (z. B. die Wiedergabe über ein Mobiltelefon, das von myPortal to go ausgelöst wird) muss die Berechtigungen der Smart VM-Ports angepasst werden. Es wird empfohlen, eine "Erlaubnisliste" für solche bekannten Nummern zu verwenden.

11.10.1 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.

Anmerkung: 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 Begrüßungen 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 Rufweitschaltung 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.

11.10.2 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 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.

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.

Anmerkung: Für die OpenScape Business Hardwaremodelle X3/X5/X8 benötigt die UC-Lösung UC Suite die UC Booster Hardware (UC Booster Card oder UC Booster Server). Bei OpenScape Business S (Softswitch) ist die UC-Lösung UC Suite bereits integriert.

Anmerkung: Nach Konfigurationsänderungen an Teilnehmern, Gruppen, Mobilitäts- oder anderen Systemparametern wie Amtskennzahlen, müssen die UC-Daten für UC Smart oder UC Suite synchronisiert werden. Die Synchronisierung erfolgt fünf Minuten nach der letzten Konfigurationsänderung. Wird die Konfiguration innerhalb der 5-Minuten-Timerfrist nochmals geändert, wird der Timer neu gestartet. Vor Beginn der Synchronisierung sind die UC-Daten also möglicherweise nicht ganz aktuell. Während der Synchronisierung sind die UC Applikation und die Web Services Interface (WSI)-API nicht verfügbar und alle verbundenen UC-Clients werden getrennt, bis die Synchronisierung der UC-Daten abgeschlossen ist. Nach Abschluss der UC-Datensynchronisation werden die Verbindungen automatisch wiederhergestellt.

12.1 Grundeinstellungen für UC Suite

Die Grundeinstellungen für UC Suite können angepasst werden.

UC Suite kann aktiviert oder deaktiviert werden. Wenn UC Suite verwendet wird, muss UC Smart deaktiviert werden.

Zusätzlich kann bei allen vom System eingeleiteten UC-Anrufen (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.

Anmerkung: Wenn CSTA-Anwendungen verwendet werden, muss der Code-Parameter für alle aktiven Leitungen eingestellt sein.

Zugehörige Tasks

[Wie Sie die IP-Adressen von Komponenten des Systems ermitteln](#)

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	Gerätetyp
Communications Client	myPortal for Desktop	PC
	myPortal for Outlook	
	myPortal @work	
	Fax Printer	
	myAttendant	
Mobile Client	myPortal to go (UC Suite) (siehe Mobility)	Smartphone, Tablet-PC
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
- Konferenzmanagement
- Aufzeichnen von Konferenzen
- Aufzeichnen von Anrufen
- Instant Messaging
- Sprach- und Faxnachrichten

12.2.2 myPortal @work

myPortal @work ist eine Unified-Communication-Anwendung, die alle benötigten Funktionen und Dienste wie komfortables Wählen über Telefonverzeichnisse, Favoriten, Gespräche und Informationen zum Anwesenheitsstatus von Kollegen zu einem zentralen Lösungskonzept vereint, um die tägliche Kommunikation zu beschleunigen, die Teamarbeit zu verbessern sowie rasch mit Kollegen, Kunden und Partnern in Verbindung zu treten.

myPortal @work kann mit beiden UC-Lösungen UC Smart und UC Suite verwendet werden. Weitere Informationen siehe [myPortal @work](#).

12.2.3 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:

- Wie Sie einen Outlook-Kontakt anrufen
- Wie Sie den Absender einer Sprachnachricht als Outlook-Kontakt anlegen
- Wie Sie eine Sprachnachricht als E-Mail senden
- Wie Sie eine Faxnachricht als E-Mail senden

12.2.4 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

12.2.5 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
- Benutzerschaltflächen
- Verwaltung von Sprach- und Faxnachrichten
- Instant Messaging
- Teamfunktionen
- Konferenzmanagement

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 Administratorrechte erforderlich. Der nutzbare Funktionsumfang ist abhängig von den verwendeten Lizenzen.

Anmerkung: 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 HFA und SIP
- OpenScape Desk Phone CP 100/200/205/400/600/600E/700/700X HFA und SIP
- OpenScape Desk Phone CP 110/210/710 HFA und SIP
- SIP-Telefone mit 3PCC-Unterstützung
- Analoge Telefone
- ISDN-Telefone
- OpenScape Personal Edition HFA und SIP
- OpenStage M3 (OpenScape Business Cordless)
- OpenScape DECT Phone S6/SL6/R6 (OpenScape Business Cordless)
- optiPoint WL3 professional SIP

Ältere Geräte (z. B. optiPoint 410/420/500, Gigaset M2/SL3/S4/SL4/S5 und optiPoint WL2 SIP) werden unterstützt. Optiset E-Geräte können nicht betrieben werden. Getestete und freigegebene Geräte entnehmen Sie bitte der Freigabemitteilung.

Anmerkung: Für den in OpenScape Desk Phone CP 400/600/600E/700/700X/710 HFA integrierten Client gelten außer der Standard-Client-Konfiguration und -Lizenz keine besonderen Voraussetzungen.

"Favoriten" im Telefonmenü enthält frei programmierbare Tasten und bezieht sich nicht auf UC-Favoriten. Details zu diesen Schlüsseln und eine Anleitung dazu finden Sie in der Gerätedokumentation.

Anmerkung: Bei analogen Telefonen und DECT-Telefonen wird die Message Waiting Indication (MWI) nicht unterstützt, die Anzeige von Informationen im Display wird nur eingeschränkt unterstützt.

Betriebssysteme

Die UC Suite PC-Clients können in Verbindung mit folgenden Betriebssystemen verwendet werden:

- Apple Mac OS X 10.10 / 10.9 / 10.8 / 10.7
- Microsoft Windows 10 / 8.1 / 8 / 7 (jeweils als 32 Bit oder 64 Bit möglich)
- Microsoft Windows Vista (32 Bit)
- Office 365 (Lokale Installation = Office 2013)

Tipp: 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 Server 2003 endet

zeitgleich mit der Betreuungseinstellung durch Microsoft. Das Produkt wird weiterhin unterstützt, jedoch nicht mehr detailliert getestet.

Die Installation unter Windows erfordert lokale Administratorrechte auf einem Client-PC, automatische Updates jedoch nicht. Die russische und 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)
- Microsoft Edge
- Mozilla Firefox Version 19 (oder neuer)
- Google Chrome

Zusätzliche Software

Zusätzliche Software	myPortal for Desktop	myAttendant	myPortal for Outlook
Oracle Java Version 8 oder höher (32 Bit / 64 Bit) oder OpenJDK 8 (32 Bit / 64 Bit)	X	X	
Microsoft Office 16 inkl. Outlook (32 Bit / 64 Bit) oder Microsoft Office 2013 / 2010 (32 Bit / 64 Bit) oder Microsoft Office 365			X
Zugriff auf Microsoft Exchange-Server (für Outlook-Kontakte und -Termine) Exchange 2015 / 2013 / 2010 (64 Bit)	X		X

Zusätzliche Software	myPortal for Desktop	myAttendant	myPortal for Outlook
Microsoft .NET Framework >= 4.0 (ab Outlook 2010)			X

Anmerkung: 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 Java in der 32 Bit Variante zu empfehlen, da somit der Arbeitsspeicher-Bedarf deutlich geringer ist. Bei allen anderen Installationen wird generell aus diesem Grund die 32-Bit-Variante von Oracle Java oder OpenJDK empfohlen.

Anmerkung: Die kontinuierliche Nutzung der bestehenden Oracle Java-Installation mit OpenScape Business erfordert keine Änderungen. Wenn ein Wechsel der Java-Version erforderlich ist (z. B. Upgrade von Oracle Java 7 auf Oracle Java 8 bzw. Open JDK Version 8), ist eine Neuinstallation des Kommunikationsclients erforderlich.

Hardware Mindestanforderungen

- 2 GHz CPU
- RAM: 2 GB
- 100 Mbit/s LAN (1 Gbit/s LAN empfohlen)
- XGA (1024x768) Bildschirmauflösung, myPortal for Outlook: SVGA (800x600) Bildschirmauflösung

Anmerkung: 4K-Monitore werden für myPortal und myAttendant nicht unterstützt.

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:

Tipp: Terminalserver- und Citrix-Server-Umgebungen inklusive Hosted Services und virtuelle Umgebungen liegen in der Verantwortung des Kunden.

Tipp: Citrix-Server-Umgebungen können einige regionale Buchstaben (z. B. deutsche Umlaute) nicht korrekt decodieren.

Betriebssysteme:

- Microsoft Windows Server 2015 (32 Bit / 64 Bit) als Microsoft Terminal Server
- Microsoft Windows Server 2012 (32 Bit / 64 Bit) als Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 (64 Bit) als Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 (64 Bit) mit Citrix XenApp 6.5 Server (Desktop Mode)

Office-Anwendungen:

- Microsoft Office 16 inkl. Outlook (32 Bit / 64 Bit)
- Microsoft Office 2013 (32 Bit / 64 Bit)
- Microsoft Office 2010 (32 Bit / 64 Bit)

Hardware-Voraussetzungen: Die Anzahl der installierbaren Clients hängt von der Server-Performance und dem zur Verfügung stehenden Arbeitsspeicher ab. 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 kann die Installationsdateien aus dem Service-Center Der Administrator kann die Installationsdateien aus dem **Service-Center** herunterladen und diese den Benutzern bereitstellen, z. B. über ein Netzlaufwerk.
- Der Administrator lädt auch das Offline-Installations-Repository aus dem Beispiel herunter.
- Der Administrator lädt auch das Offline-Installations-Repository aus dem **Service-Center** herunter und die Clients können offline installiert werden.

12.2.7 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.

Anmerkung: Beachten Sie bitte unbedingt die Hinweise in der Datei `ReadMe first.rtf`.

Silent Installation/Deinstallation 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
<code>/quiet</code>	Startet den Installationsvorgang ohne Benutzeroberfläche und ohne Eingreifen des Benutzers. Dieser Parameter erfordert, dass das Repository schon gefunden wurde.
<code>/repository</code>	Legt die IP-Adresse oder den Hostnamen für die Installation fest. Zum Beispiel: <code>/repository=192.168.50.50</code>
<code>/installpath</code>	Legt den Pfad der installierten Clients fest. Der voreingestellte Wert lautet: <code>C:\Program Files(x86)\communicationsclients\</code>
<code>/autostart</code>	Startet den Installationsvorgang ohne Eingreifen des Benutzers. Dieser Parameter erfordert, dass das Repository schon gefunden wurde.
<code>/i</code>	Wählt das zu installierende Produkt aus. Verfügbare Werte sind <code>OLI</code> , <code>myPortal</code> , <code>myAgent</code> , <code>FPD</code> , <code>myReports</code> und <code>all</code> . Zum Beispiel: <code>/i="OLI,FPD"</code>
<code>/u</code>	Wählt das zu entfernende Produkt aus. Zum Beispiel: <code>/u="OLI,FPD"</code>
<code>/set</code>	Wählt die Produkte aus, die im System installiert werden sollen. Dieser Schalter installiert die gewählten Produkte oder ändert bereits installierte Produkte. Es werden auch installierte Produkte entfernt, die nicht angegeben wurden. Zum Beispiel: <code>/set="OLI,FPD"</code>
<code>/repair</code>	Repariert die angegebenen Produkte. Zum Beispiel: <code>/repair="OLI,FPD"</code>

12.2.8 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 geschlossen werden muss/müssen, um das Update durchzuführen.

Anmerkung: Es wird empfohlen, die angebotenen Updates stets durchzuführen. Dies gilt ebenso für Software, die für bestimmte UC-Clients erforderlich ist.

Anmerkung: Automatische Updates von myPortal @work werden in MacOS nicht unterstützt.

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.

Anmerkung: Circuit-Benutzer sind im Benutzerverzeichnis nicht sichtbar, da keine Lizenz pro Nutzer zugeordnet ist.

Im Benutzerverzeichnis werden zu jedem Benutzer folgende Informationen angezeigt:

- Symbol für Anwesenheitsstatus

Der Administrator kann den Anwesenheitsstatus für jeden Benutzer ändern.

- **Nebenstelle**
- **Benutzername**

Anmerkung: UCSuite erlaubt und unterstützt zwar die Änderung von Benutzernamen für die eigenen Clients, dennoch könnten solche Änderungen

die Anmeldung von Nicht-UCSuite-Clients wie myPortalToGo/myPortal@Work (wo zutreffend) beeinträchtigen und werden daher in solchen Situationen nicht empfohlen.

- **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.
- **Voicemail**
Der Benutzer kann Sprachnachrichten empfangen.
- **Anrufumleitung**
Für den Benutzer ist eine Anrufumleitung konfiguriert.

Suchfunktionalität sind auch für die Benutzerverzeichnisfelder verfügbar.

Folgende Einstellungen können konfiguriert werden:

Werte und Einstellungen	Stichworte
Persönliche Daten	
Eigene persönliche Daten	Eigener Name, Benutzername, Kennwort, E-Mail-Adresse, Abteilung, Zusätzliche Rufnummer
Eigenes Bild	Eigenes Bild Unterstützte Dateiformate: BMP, JPG/JPEG/JFIFI, PNG Max. Dateigröße: 10MB
Benutzerebene	Empfang von Sprachnachrichten: siehe Teilnehmer Benutzer als Vermittlungsplatz: siehe Teilnehmer Benutzer als Agent: siehe Teilnehmer
Meine Einstellungen	
Darstellung	Skin-Farben, Sprache der Benutzeroberfläche
Benachrichtigungen	Pop-up-Fenster
Kalender-Anbindung	Automatische Erstellung von Outlook-Terminen bei Abwesenheit, Automatische Aktualisierung des Anwesenheitsstatus durch Outlook-/iCal-Termine

Werte und Einstellungen	Stichworte
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	Aufzeichnungsmodus oder Ansagemodus, Sprache der Sprachbox
Sprachnachricht-Benachrichtigung	Benachrichtigungsdienst für Nachrichten
Fax-Benachrichtigung	Benachrichtigungsdienst für 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
Sichtbarkeit des Anwesenheitsstatus	Sichtbarkeit Ihres Anwesenheitsstatus für Andere
VoiceMail-Anwesenheitsstatus	Ansage Ihres Anwesenheitsstatus für externe Anrufer, Ansage Ihres Anwesenheitsstatus für bestimmte Anrufer
Andere Benutzer können mein BLF-Layout kopieren	Andere Benutzer können die BLF-Gruppen und -Tasten kopieren Diese Option ist für bereits erstellte Profile nicht verfügbar.
myAttendant	
LAN-Nachrichten	Textbaustein für Sofortnachrichten
DuWas	MSN
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 Kennwort für UC Clients ist standardmäßig sechsstellig. Die Länge des Kennworts kann an den eigenen Bedarf angepasst werden (6-10 Stellen). Dasselbe Zeichen darf höchstens zweimal hintereinander stehen und es sind höchstens drei aufeinanderfolgende Zeichen nacheinander zulässig. Der Benutzerkontoname (in umgedrehter sowie tatsächlicher Reihenfolge) kann nicht Teil des Kennworts sein und für die Kennwortänderung muss das alte Kennwort bekannt sein. Der Benutzer muss nach der ersten Verwendung das Standardkennwort ändern. Die maximale Anzahl fehlerhafter Anmeldeversuche beträgt fünf. Ein Administrator mit dem Profil **Advanced** kann das Kennwort eines Benutzers ändern (z.B. falls es der Benutzer vergessen hat).

Anmerkung: Vor- und Nachname eines Benutzers werden im Benutzerverzeichnis 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 Expertenmodus angezeigt werden, nicht überschrieben. In diesem Fall existieren zwei unterschiedliche Benutzernamen für denselben Benutzer. Wenn der Vorname und der Nachname insgesamt länger als 16 Zeichen sind, erfolgt eine Kürzung auf 16 Zeichen, damit der Name am Display angezeigt werden kann.

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.

Teilnehmerdaten zurücksetzen

Die Einstellungen eines Benutzers können auf Standardwerte zurückgesetzt werden. Durch das Zurücksetzen von Benutzerdaten werden alle Benutzerdaten gelöscht, einschließlich Vorname, Nachname und Anmeldename.

Unabhängig davon, ob der Vor- oder Nachname eines Benutzers über **WBM > Expertenmodus > Telephony Server > Teilnehmer** eingestellt wurde, führt das Zurücksetzen dieses Benutzers über UC Suite letztlich auch zur Zuweisung der Nummer, die als Durchwahl gespeichert ist, im Feld **Name**.

12.3.2 Benutzer-Profile der 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 zugeordnete Profil - löschen den Benutzer automatisch aus dem Profil.

Wenn die Zuordnung eines Benutzers zu einem Profil aufgehoben wird, behält er die durch das Profil dargestellten Einstellungen bei.

Wenn ein Benutzer bereits einem Profil zugeordnet ist, werden nur Änderungen in den gesperrten Profilelementen auf diesen Benutzer angewendet. Wenn das Sperrsymbol entsperrt ist, gelten die Änderungen nicht.

Wenn ein gesamtes Profil gelöscht wird, behalten Benutzer, die diesem Profil zugeordnet sind, ebenfalls die Profileinstellungen bei.

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 Benutzeroberfläche
Benachrichtigungen	Popup-Fenster
Outlook-Anbindung	Automatische Erstellung von Outlook-Terminen bei Abwesenheit, Automatische Aktualisierung des Anwesenheitsstatus durch Outlook-/iCal-Termine
Abkürzungstasten	Aktivierung und Einrichtung von Tastaturkombination für den Zugriff auf verschiedene, häufig verwendete Funktionen über die Tastatur. Das Schlosssymbol legt fest, ob der Benutzer diese Einstellungen selbst ändern kann.
Verschiedenes	Automatisches Zurücksetzen des Anwesenheitsstatus, Übergabemethode, Aufbewahrungsdauer für Journaleinträge, Serveradresse
Anrufregeln	
Anrufweiterleitungsziele	Statusbezogene Anrufumleitung
Kommunikation	
Einstellungen für Sprachnachrichten	Aufzeichnungsmodus oder Ansagemodus, Sprache der Sprachbox
Sprachnachricht-Benachrichtigung	Benachrichtigungsdienst für Nachrichten
Fax-Benachrichtigung	Benachrichtigungsdienst für Nachrichten

Menüpunkte	Werte und Einstellungen zu
Benachrichtigungen über entgangene Anrufe	Benachrichtigungsservice für entgangene Anrufe
Profile	
Profile	Profil für persönlichen AutoAttendant. Verfügbarer Status: Besetzt, Nicht angenommen, Besprechung, Krank, Pause, Außer Haus, Urlaub, Mittagspause, Zu Hause
Sensibilität	
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
Favoriten	
Favoriten	Favoritengruppen mit einer Liste von Kontakten, die dem Benutzer zugewiesen werden können.

Weitere Informationen zu Einstellungen der Benutzer-Profile finden Sie in den Bedienungsanleitungen der UC Clients unter den in der Tabelle aufgeführten Stichworten.

12.4 Anwesenheitsstatus und CallMe-Dienst

Anwesenheitsstatus und CallMe-Dienst zeigen und optimieren die Erreichbarkeit von Teilnehmern. Der Anwesenheitsstatus ermöglicht eine einfache statusbezogene Anrufumleitung sowie eine mit myPortal for Desktop bzw. myPortal for Outlook flexibel konfigurierbare regelbasierte Anrufumleitung.

12.4.1 Anwesenheitsstatus (Präsenz)

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** können Sie den Zeitpunkt der geplanten Rückkehr zu **Büro** bzw. **CallMe** festlegen.

Als Teilnehmer können Sie folgende Status auswählen:

- **Büro**
- **Besprechung**
- **Krank**
- **Pause**
- **Außer Haus**
- **Urlaub**
- **Mittagspause**
- **Zu Hause**
- **Anrufschutz**

Anmerkung: Der Systemadministrator kann die Sichtbarkeit des Status „krank“ innerhalb der Systemadministration ein- und ausschalten. Siehe [OpenScape Business UC Suite > Server](#)

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 den Anrufer durch statusbezogene Ansagen über die Art der Abwesenheit und den geplanten Zeitpunkt der 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.

Anmerkung: Sichtbarkeitseinstellungen werden nicht auf myAttendant-Benutzer angewendet, da diese immer den Anwesenheitsstatus anderer Benutzer sehen können.

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.

Anmerkung: 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 der Anwesenheitsstatus zur Beginn- und Endzeit des betreffenden Termins automatisch. Die Prüfung des Kalenders auf Termine erfolgt in Intervallen von 30 s.

Anmerkung: 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.

Anmerkung: Der Anwesenheitsstatus "krank" ist je nach Systemeinstellung des Administrators möglicherweise nicht verfügbar.

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 dem 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 Ende-Zeit 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.

Anmerkung: 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.

Pop-up-Fenster bei Änderung des Anwesenheitsstatus

Sie können als Teilnehmer Änderungen Ihres Anwesenheitsstatus durch Pop-up-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.

Anmerkung: Falls für das gesteuerte Endgerät das Leistungsmerkmal sofortige Rufumleitung aktiviert ist, empfängt der Application Launcher keine anrufbezogenen Ereignisse vom Kommunikationsserver

und kann deshalb auch keine Applikationsanreize erzeugen. Gleiches gilt auch für den Fall, das das UC Suite Leistungsmerkmal CallMe aktiviert ist.

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.

Anmerkung: Bei Einwahl oder Anrufen in einer offenen Konferenz sollte die CallMe-Funktion nicht verwendet werden.

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 unbekanntem Kontakten an seine Sprachbox.

Darüber hinaus unterstützt die regelbasierte Anrufumleitung:

- beliebige Ziele
- Anwesenheitsstatus (**Büro, Besprechung, Krank, Pause, Außer Haus, Urlaub, Mittagspause, Zu Hause**)

Anmerkung: CallMe und DND gelten nicht für die regelbasierte Anrufumleitung.

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 "**Regel aktiv**" 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

UC Suite

Verzeichnisse und Journal

- (außer) zwischen einer bestimmten Start- und Ende-Uhrzeit

12.5 Verzeichnisse und Journal

Verzeichnisse, die Favoritenliste und das Journal organisieren Kontakte und Anrufe.

12.5.1 Verzeichnisse

Verzeichnisse organisieren die Kontakte der Teilnehmer. Teilnehmer können mit UC Suite Clients sowie mit Systemtelefonen mit Display auf die Kontakte zugreifen.

Das System stellt folgende Verzeichnisse mit den folgenden Funktionen und folgender Prioritätsreihenfolge für die Rufnummernsuche bereit (Nummernsuche wird nur für externe Anrufe unterstützt, und für den Fall, dass Amt bzw. ITSP den Namen nicht bereitstellen):

Verzeichnis	myPortal for Desktop, my Attendant, myAgent, 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.	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.	-	Über den persönlichen Assistenten importierte Outlook-Kontakte.

Verzeichnis	myPortal for Desktop, my Attendant, myAgent, Fax Printer	myPortal for Outlook	Systemtelefon mit Display
Internes Verzeichnis	<p>Das interne Verzeichnis von UC Smart bietet mit UC Suite zusätzliche Leistungsmerkmale. Er beinhaltet:</p> <ul style="list-style-type: none"> • Alle internen Teilnehmer • Gruppen, für die das Anzeigen im System aktiviert ist • Zusätzliche Telefonnummern, wenn der Teilnehmer diese Informationen für andere interne Teilnehmer sichtbar gemacht hat <p>Interne Teilnehmer (mit Systemtelefon) werden mit Anwesenheitsstatus dargestellt und können per Instant Messaging kontaktieren 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 Lesezugriff auf dieses Verzeichnis.</p> <p>Das interne Verzeichnis enthält das Systemverzeichnis. Suchvorgänge im internen Verzeichnis umfassen aber keine Ergebnisse aus dem Systemverzeichnis, sondern nur Einträge des internen Verzeichnisses.</p>		Enthält alle internen Teilnehmer und Gruppen, für die 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)	<p>Enthält die Kontakte des öffentlichen Exchange-Ordners, falls vom Administrator konfiguriert. Diese werden im Externen Verzeichnis angezeigt.</p> <p>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.</p>		-
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.		

Verzeichnis	myPortal for Desktop, my Attendant, myAgent, Fax Printer	myPortal for Outlook	Systemtelefon mit Display
Systemverzeichnis	Enthält alle Systemnummern, UC- und Nicht-UC-Benutzer. Nicht-UC-Benutzer sind Teilnehmer ohne UC-Lizenzen und virtuelle Teilnehmer wie Fax, AutoAttendant. Das Systemverzeichnis gilt nicht für den Faxdrucker		Enthält alle internen Teilnehmer und alle zentralen Kurzwahlnummern. Der Administrator kann die Anzeige eines Teilnehmers im Systemtelefonbuch aktivieren und deaktivieren.

Anmerkung: Telefonnummern, die in den Benutzereinstellungen und allen Verzeichnissen (intern, extern, persönlich, Outlook, Exchange) gespeichert sind, sollten im kanonischen Format eingegeben werden, um sowohl von UC als auch vom Gerät aus erreichbar zu sein.

Der Zugangscode darf nicht in der Nummer enthalten sein.

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 ganzen Wörtern 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 wahlweise in den Feldern **Titel**, **Vorname**, **Nachname**, **Firma**, **Durchwahl**, **Firmen-Rufnr.**, **Geschäftlich 1**, **Geschäftlich 2**, **Privat 1**, **Privat 2**, **Mobilrufnummer** und **E-Mail** suchen und die maximale Anzahl von Treffern begrenzen. Die moderne Oberfläche von myPortal for Desktop unterstützt die erweiterte Suche nicht. In einem Gerät werden nur **Geschäftlich 1**, **Privat 1**, **Mobilrufnummer** unterstützt.

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.

12.5.2 Internes Verzeichnis

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.

12.5.3 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.
- Zu Hause
- Faxnr.
- E-Mail

- Ort

Anmerkung: Der Name des Kontakts wird in der Anrufliste nur angezeigt, wenn Sie sowohl das Feld Vorname als auch das Feld Nachname ausfüllen.

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.

Anmerkung: 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**.

12.5.4 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.

Anmerkung: 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.

12.5.5 Systemverzeichnis

Mit Blick auf UC Suite Clients enthält das Systemverzeichnis alle Systemnummern für UC- und Nicht-UC Benutzer. Nicht-UC-Benutzer sind Teilnehmer ohne UC-Lizenzen und virtuelle Teilnehmer wie Fax, AutoAttendant. In Bezug auf Geräte enthält das Systemverzeichnis alle internen Teilnehmer und alle zentralen Kurzwahlnummern.

Der Administrator kann die Anzeige für jeden Teilnehmer bzw. jede Kurzwahlnummer mit Namen individuell deaktivieren.

12.5.6 Unified-Verzeichnis

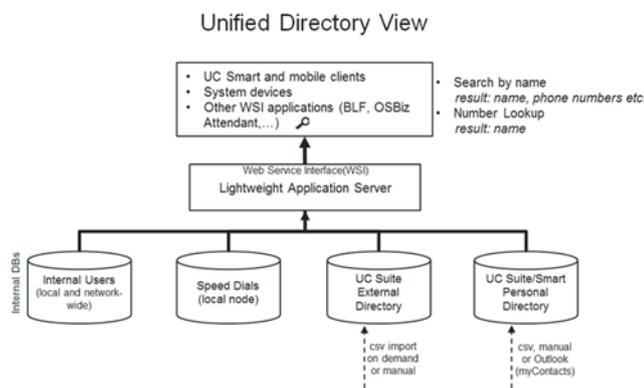
OpenScape Business bietet verschiedene Datenquellen zum Speichern und Abrufen von Teilnehmer- oder Kontaktdaten – von internen Teilnehmerdaten in der internen Benutzerkonfiguration über die

interne Kurzwahlliste bis hin zu den verschiedenen Verzeichnissen der UC-Anwendungen.

Jede Datenquelle in OpenScape Business wird von einer bestimmten Client-Anwendung verwendet, die entweder Teil der Systemsoftware auf den Telefongeräten oder Teil einer UC-Client-Anwendung ist. Abhängig von den verwendeten Datenquellen und Clients werden die Daten unterschiedlich abgerufen und dargestellt.

Der Unified-Verzeichnisdienst in OpenScape Business nutzt die bestehenden OpenScape Business-Datenquellen für die Funktionen Rufnummernsuche und Namensauflösung. Er übermittelt an alle Systemgeräte und OpenScape Business-Clients einheitliche Suchergebnisse und Namensauflösungsinformationen.

Der Zugriff auf den Unified-Verzeichnisdienst kann entweder über das Web Service Interface (WSI) mit externen Clients wie myPortal to go oder intern über Anrufbearbeitungsmechanismen (z. B. von OpenStage-Telefonen) erfolgen.



Der Unified-Verzeichnisdienst verwendet die folgenden internen Datenbanken und Verzeichnisse von OpenScape Business:

- Internes Benutzerverzeichnis (netzweit)
- Kurzwahllisten
- UC Smart Persönliches Verzeichnis (optional)
- UC Suite Externes Verzeichnis (optional)
- Persönliche Outlook-Kontakte (falls importiert über myContacts)

Der Unified-Verzeichnisdienst ist auf allen Knoten eines OpenScape Business-Systems ab V2R2 verfügbar. Es erfordert keine spezielle Hardware, Software oder zusätzliche Lizenzen.

Um bei der Verwendung des Unified-Verzeichnisdienstes die besten Ergebnisse zu erzielen, sollten Sie einige Regeln für Rufnummernformate und zur Schreibweise von Namen beachten.

12.5.6.1 Leistungsmerkmale

Unterstützte Geräte/Clients

Der Unified-Verzeichnisdienst stellt folgende Funktionen bereit:

- Telefonbuchsuche in mehreren internen Datenquellen von OpenScape Business

- Einheitliche Bereitstellung des Suchergebnisses für alle unterstützten Kunden
- Rufnummernsuche / Namensauflösung in mehreren internen Datenquellen
- Einheitliche Bereitstellung der Namensauflösungsergebnisse für alle unterstützten Clients
- Externer Datenzugriff über die WebServices-Schnittstelle (WSI)

Die Leistungsmerkmale sind für Einzelknotensysteme wie folgt verfügbar. In OpenScape Business-Netzwerken hängt die Verfügbarkeit der Features hauptsächlich von der Art der Verbindung der Amtsleitungen, Geräte und Clients innerhalb des Netzwerks ab.

Unified Directory unterstützt folgende Clients/Systemgeräte von Unify unter Verwendung der angegebenen Schnittstellen:

Gerät/Client	Verwendete(s) Schnittstelle/Protokoll	Hinweise
OpenStage-Telefone	Anrufverarbeitung/ HFA-Protokoll	WSI/HTTP(S) ist optional für OpenStage 60/80 für Anrufer-Bilder
OpenScape DeskPhone IP	Anrufverarbeitung/ HFA-Protokoll	WSI/HTTP(S) ist optional für DeskPhone IP 55 für Anrufer-Bilder
Schnurlose (CMI)-Geräte	Anrufverarbeitung/ CMI-Protokoll	
CP 100/110/200/210	Anrufverarbeitung/ HFA-Protokoll	
DeskPhone CP400/ 600/600E/ 700/700X/710	WSI/HTTP(S)	
myPortal @work	WSI/HTTP(S)	
myPortal to go	WSI/HTTPS	
OpenScape Business Attendant/BLF	Anrufverarbeitung/ CorNet-Protokoll	WSI/HTTP(S) ist optional

Anmerkung: Die UC Suite myPortal-, myAttendant- und myAgent-Clients verwenden eigene Mechanismen für die Verzeichnissuche und Namensauflösung.

Suchfunktion

Die Unified Directory-Suche wird immer unter Verwendung der spezifischen Geräte-/Client-Benutzerschnittstelle durchgeführt. Die Suchkriterien und der verwendete Zeichensatz können abhängig von den verwendeten Clients eingeschränkt sein.

Nach Eingabe des Suchkriteriums wird die Suche in den nachfolgenden Verzeichnissen durchgeführt

- Internes Benutzerverzeichnis (netzwerkweit)
- Kurzwahllisten
- UC Smart Persönliches Verzeichnis (optional)
- UC Suite Externes Verzeichnis (optional)
- Persönliche Outlook-Kontakte (falls über myContacts importiert)

Alle Übereinstimmungen innerhalb der obigen Verzeichnisse werden zusammen mit ihrer Herkunft als Suchergebnisse angezeigt. Die Übereinstimmungen enthalten entweder den vollständigen Kontaktdatenatz oder nur Teile davon. Die Informationstiefe der Ergebnisse hängt von der Datenquelle ab.

Anmerkung: Die Suche nach Gruppennamen in myPortal @work wird im UC Suite-Modus nicht unterstützt. Es wird nur die Suche nach lizenzierten Benutzern (Basislizenz) und lizenzierten MULAP-Gruppen (UC-Einträge) unterstützt.

Die Übereinstimmungen werden auf den Geräten oder Clients angezeigt, abhängig von den Anzeigefähigkeiten.

	Internes Benutzerv	Kurzwahl	UC Smart Persönlich Verzeichn	UC Suite Externes Verzeichn	Persönliche Outlook-Kontakte (über myContacts)
Nachname	X	---	X	X	X
Vorname	X	---	X	X	X
Kurz-/Anzeigename	X	X	---	---	---
Büro-Rufnr.	---	---	X	X	X
Private/ext. Rufnr.	---	---	X	---	X
Mobilrufnr.	---	---	X	X	X
E-Mail-Adr.	---	---	X	X	X
Firmenname	--	---	X	X	X
Ort	---	---	---	---	---
Kontaktbild	---	---	X	---	X
Kontaktbildvorschau	---	---	X	---	X

Rufnummernsuche

Mit der einheitlichen Rufnummernsuche wird der Anrufer (CLI) durch eine Nummernsuche in allen unterstützten internen Datenquellen aufgelöst. Die Suche wird in den folgenden Rufnummer-Feldern durchgeführt:

- Büro-Rufnummer

- Mobilrufnummer
- Private Rufnummer

Die Rufnummernsuche wird im Allgemeinen bei eingehenden oder ausgehenden Anrufen ausgelöst, wobei bestimmte Routing- und Weiterleitungsfunktionen zusätzlich berücksichtigt werden.

Eine feste Priorisierung der Datenquellen, die für die Rufnummernsuche verwendet werden, wird implementiert, um so schnell wie möglich ein Ergebnis zu erhalten. Das Ergebnis enthält entweder nur den Nachnamen, den Vornamen, den Anzeigenamen oder, sofern verfügbar, die vollständigen Kontaktdaten.

Tabelle 7: Unterstützte Datenquellen und Priorisierung

Priorität	Datenquellen	Bemerkung
1	CO ITSP Name (wie vom Provider gesendet)	Voraussetzung ist, dass das Flag "Name im Amt" aktiviert wird.
2	Kurzwahlliste	
3	Persönliche Kontakte	
4	UC-Benutzerdetails	

Die abgerufenen Daten werden auf dem Gerät des Benutzers und/oder im UC-Client angezeigt. Die Informationstiefe der Ergebnisse hängt von den Anzeigefähigkeiten ab.

• **Kommende Rufe**

Unterstütztes Szenario für Einzelknotensysteme:

- Basic Call
- Gruppenruf/MULAP-Ruf
- Rufzuschaltung
- Einzelschritt-Übergabe (SSCT)
- Gespräch übergeben/Übergabe nach Melden/Rückfrage
- Uneingeschränkte Gesprächsumleitung (CFU)
- Verzögerte Anrufumleitung (CFNR = Call Forwarding No Reply)
- Anrufumleitung bei Besetzt (CFB = Call Forwarding Busy)
- Übergabe ohne Rückfrage
- Anrufübernahme

Anmerkung: Anrufübernahme unterscheidet sich von Anrufübernahmegruppe. Wenn in der Anrufübernahmegruppe eine externe Nummer im Unified Directory gespeichert ist, wird der Name des Anrufers von den Mitgliedern der Gruppe nicht angezeigt.

Unterstütztes Szenario für mehrere Knoten (Netzwerk). Szenario ist ein Gateway-Anruf.

• **Gehender Anruf**

Im Falle eines ausgehenden Anrufs erfolgt die Rufnummernsuche für die gewählte Teilnehmernummer nur einmal.

Unterstütztes Szenario für Einzelknotensysteme ist ein Basic Call an eine externe Rufnummer.

Die Darstellung der Rufnummer-Suchergebnisse hängt von den Anzeigefähigkeiten der Telefone ab.

12.5.6.2 Regeln und Konventionen

Bei den Rufnummern- und Namensformaten innerhalb der Datenquellen sind einige Konventionen zu beachten, um optimale Ergebnisse mit dem Unified-Verzeichnisdienst zu erhalten.

Unterstütztes Rufnummernformat

Alle externen Rufnummern innerhalb der Datenquellen müssen einschließlich Länder- und Ortsvorwahl im kanonischen Format eingegeben werden, z. B. +4989700712345

Die Kurzwahlliste unterstützt nur das vom System wählbare Format (z.B. 0089700712345 oder 0004989700712345)

Wenn Kurzwahlnummern so konfiguriert sind, dass sie über LDAP zugänglich sind, müssen Sie die Option zur Nummernkonvertierung aktivieren, um den Kontaktnamen anzuzeigen, wenn die Nummer im kanonischen Format vorliegt. Weitere Informationen zum Aktivieren der Nummernkonvertierung finden Sie unter [Wie Sie eine externe Datenquelle für Open Directory Service hinzufügen](#).

Unterstützte Namensformate

Bei Namensformaten und Zeichensätzen sind die folgenden Konventionen zu beachten:

- **Namensformat bei Kurzwahl**

Die Namenssuche innerhalb der Kurzwahlliste wird nur in Kombination mit bestimmten Konfigurationsregeln unterstützt. Vor- und Nachname müssen im vorhandenen Namensfeld nach dem folgenden Muster eingegeben werden:

<Nachname>, <Vorname> (kommagetrennt)

- **Interne Teilnehmer bei Migrationsszenarien**

Bei internen Teilnehmern, die diese Konfigurationsregeln nicht beachten, wird eine Migration auf V2R1 und höher ggf. unerwartete Folgen und wird nicht ordnungsgemäß unterstützt. Dies bedeutet, dass der Administrator interne Namen vor Durchführung der Migration in das folgende Format konvertieren sollte:

<Nachname>, <Vorname> (kommagetrennt)

Verfügbarkeit von Verzeichnisänderungen

Nach dem Erstellen, Aktualisieren oder Löschen von Kontakten in den verschiedenen Datenquellen kann es bis zu 10 Minuten dauern, bevor alle Änderungen in den Suchergebnissen sichtbar sind.

12.5.6.3 Funktionale Grenzen

Für Unified-Verzeichnisse gelten die folgenden funktionalen Grenzen:

Namenssuche

- Unterstützung von Gruppennamen

Gruppennamen (nicht MULAP-Namen) können zurzeit nicht in allen Arten von Konfigurationen durchsucht werden

- Unterstützung von Sonderzeichen

Auf den meisten Telefongeräten kann der Benutzer nur nach den Standardzeichen "a-z" suchen. Die Eingabe von (diakritischen) Sonderzeichen (wie z.B. der deutschen Umlaute Ää, Öö, Üü oder ß) ist über die Benutzeroberfläche des Telefongeräts nicht möglich.

Daher beinhaltet ein Suchergebnis mit einfachen Zeichen auch Sonderzeichen. Bei einer Suche mit den Zeichen „acdegilnorstuyz“ sind auch die entsprechenden Sonderzeichen "àáâãäå#äçćčďđèéêëëë#ìíîíłńñňòóôõöőřśšţùúûüýÿžžž" im Suchergebnis enthalten.

Anmerkung: Eine Suche im Telefonbuch mit Platzhalterzeichen am Anfang des Suchbegriffs, z. B. <*jo*>, wird nur für interne Benutzer unterstützt.

- Unterstützung von Kurzwahlnamen

Die Namenssuche innerhalb der Kurzwahlliste wird nur in Kombination mit bestimmten Konfigurationsregeln unterstützt. Vor- und Nachname müssen im vorhandenen Namensfeld nach einem der folgenden Muster eingegeben werden

- <Nachname>, <Vorname> (kommagetrennt)
- <Nachname>, <Vorname> (Leerschritt als Trennzeichen)

Namensanzeige

Persönliche Kontakte aus UC Smart und dem externen Offline-Verzeichnis, bei denen Vorname und Nachname zusammen länger als 24 Zeichen sind, werden zwecks Anzeige auf dem Gerätedisplay auf 24 Zeichen gekürzt.

Rufnummernsuche

Die Funktion Rufnummernsuche (Kontaktname aus Rufnummer des Anrufers ermitteln) wird vom Unified-Verzeichnisdienst für SIP- und S0-Geräte nicht unterstützt.

12.5.6.4 Unified-Verzeichnis in vernetzten Systemen

Der Unified-Verzeichnisdienst ist auf allen Knoten eines OpenScape Business-Netzwerks aktiv und nutzt die Datenquellen des eigenen Systems. Telefongeräte und Clients verwenden innerhalb ihres eigenen Knotens immer den Unified-Verzeichnisdienst.

Es kommt daher auf die Art des Datenquelleninhalts an, ob netzweite Kontakte verfügbar sind oder nicht.

Tabelle 8: Lokale und netzweite Datenquellen

Datenquelle	Lokale Daten	Netzweite Daten
Internes Benutzerverzeichnis	X	X
Kurzwahllisten	X	---
UC Smart Persönliches Verzeichnis	X	---
UC Smart Persönliches Verzeichnis	X	---
Persönliche Outlook-Kontakte (über myContacts)	X	---

Rufnummernsuche

In Vernetzungsszenarien wird die Funktion Telefonnummer suchen nicht verwendet. In solchen Fällen wird der Name über normale Vernetzungsmechanismen zwischen den Netzknoten übertragen.

Für interne Teilnehmer wird der konfigurierte Anzeigename verwendet, so dass eine Suche nicht erforderlich ist.

12.5.7 Abteilungen

Abteilungen gruppieren Teilnehmer im internen Verzeichnis nach ihrer organisatorischen Zugehörigkeit. Das interne Verzeichnis ermöglicht die Suche bzw. Sortierung nach Abteilung.

12.5.8 Favoritenliste

In der Favoritenliste haben Sie als Teilnehmer ausgewählte Kontakte stets im Blick. Diese können Sie besonders einfach anrufen. Sie sehen alle internen Teilnehmer mit Systemtelefon sowie externe Kommunikationspartner 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.

12.5.9 Journal

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 die von Ihnen unbeantworteten entgangenen Anrufe, bei denen eine Rufnummer übermittelt wurde. Sobald einer dieser Anrufe beantwortet wird, werden alle Einträge mit der entsprechenden Rufnummer von der Liste gestrichen.

- **All Anrufe**
- **Entgangen**
- **Angenommen**
- **Intern**
- **Extern**
- **Ankommend**
- **Gehend**
- **Zeitlich geplant**

Enthält die von Ihnen als Teilnehmer zu bestimmten Terminen geplanten Anrufe. Das Leistungsmerkmal „Geplante Anrufe“ steht für Agenten des 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 evtl. anstehende geplante Anrufe hin. Beim Starten informiert myPortal for Desktop oder myPortal for Outlook Sie über evtl. 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.

Beim Start der modernen Benutzeroberfläche myPortal for Desktop werden nur 100 Journaleinträge geladen. Danach und wenn neue Anrufe eingehen, überschreitet die Nummer in der Anrufliste 100 Einträge.

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.

Anmerkung: In der Aufbewahrungsdauer wird auch der maximale Zeitraum für Auswertungen mit myReports festgelegt.

Gruppierung nach Zeitraum

Die Anrufe sind in jeder Gruppe zeitlich gruppiert, z.B.: Heute, Gestern usw., Letzte Woche, Letzten Monat und Älter. Ihr Administrator kann festlegen, wie lange Anrufe im Journal gespeichert bleiben. Nach dieser festgelegten Zeit werden Einträge automatisch gelöscht. In der modernen Benutzeroberfläche von myPortal for Desktop steht die Gruppierung nach Zeitraum nicht zur Verfügung.

Gesprächsdaten

Jeder Anruf wird mit Datum und Zeit angezeigt und sofern vorhanden mit der Rufnummer. Falls ein Verzeichnis zur Rufnummer weitere Informationen wie **Nachname**, **Vorname** und **Firma** enthält, werden auch diese angezeigt. Zusätzlich werden in den meisten Ordnern die Spalten **Richtung**, **Dauer** und **Gespräch abgeschlossen** angezeigt. In der modernen Benutzeroberfläche von myPortal for Desktop stehen nicht alle Gesprächsdaten zur Verfügung.

Sortierung

Sie können die Anrufe im Journal nach Spalten 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 die Suche eingrenzen. 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 myPortal for Outlook als CSV-Datei exportieren:

12.6 Anrufe

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 kann die Wahl noch abgebrochen werden. Wird der voreingestellte Wert von 3s auf 0s geändert, wird die Wahl sofort ausgeführt. Der Wert wird in den Einstellungen der UC Suite Clients geändert.

Windows-Anwendungen, die mittels Windows-Standardkomponenten implementiert wurden, unterstützen in der Regel Desktop-Wahl und Clipboard-Wahl, nicht jedoch 16-bit-Anwendungen. Desktop-Wahl wird nur von 32 Bit Applikationen unterstützt.

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.

Tipp: Sie müssen der 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 und Einleiten einer Konferenz wird eine laufende Aufzeichnung abgebrochen.

Anmerkung: DTMF wird während der Anrufaufzeichnung nicht unterstützt.

12.7 Konferenzen

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
Verwendung	<ul style="list-style-type: none"> • Telefongesteuert • Applikationsgesteuert 	<ul style="list-style-type: none"> • Applikationsgesteuert 	<ul style="list-style-type: none"> • Applikationsgesteuert 	<ul style="list-style-type: none"> • Applikationsgesteuert
Beginn	<ul style="list-style-type: none"> • Manuell 	<ul style="list-style-type: none"> • Geplant 	<ul style="list-style-type: none"> • Manuell 	<ul style="list-style-type: none"> • Manuell
Ende	<ul style="list-style-type: none"> • Manuell 	<ul style="list-style-type: none"> • Geplant • Manuell 	<ul style="list-style-type: none"> • Manuell 	<ul style="list-style-type: none"> • Manuell

	Ad-hoc	Geplant	Permanent	Offen
Dauer der Reservierung von Konferenzkanälen	<ul style="list-style-type: none"> Standardmäßig 1 Stunde 	<ul style="list-style-type: none"> Geplant 	<ul style="list-style-type: none"> Bis zur Deaktivierung oder Löschung der Konferenz 	<ul style="list-style-type: none"> Bis zur Deaktivierung oder Löschung der Konferenz
Nebenstelle	x	x	-	-
Wiederholung	<ul style="list-style-type: none"> Manuell 	<ul style="list-style-type: none"> Geplant 	-	-
Richtung des Verbindungsaufbaus aus Sicht des Systems	<ul style="list-style-type: none"> Gehend 	<ul style="list-style-type: none"> Gehend Ankommend 	<ul style="list-style-type: none"> Ankommend 	<ul style="list-style-type: none"> Ankommend
Teilnehmerkreis	<ul style="list-style-type: none"> Fest 	<ul style="list-style-type: none"> Fest 	<ul style="list-style-type: none"> Fest 	<ul style="list-style-type: none"> Offen
Authentifizierung der Konferenzteilnehmer	-	<ul style="list-style-type: none"> Individuelle Konferenz-ID (optional) Passwort (optional) 	<ul style="list-style-type: none"> Individuelle Konferenz-ID (optional) Passwort (optional) 	<ul style="list-style-type: none"> Gemeinsame Konferenz-ID (optional)
Aufzeichnung, sofern im System aktiviert	<ul style="list-style-type: none"> Manuell (On Demand Conference Recording) 	<ul style="list-style-type: none"> Automatisch (Auto Conference Recording) Manuell (On Demand Conference Recording) 	<ul style="list-style-type: none"> Automatisch (Auto Conference Recording) Manuell (On Demand Conference Recording) 	<ul style="list-style-type: none"> Automatisch (Auto Conference Recording) Manuell (On Demand Conference Recording)
Einladung per E-Mail mit:	<ul style="list-style-type: none"> Name der Konferenz Link für Web Collaboration Sitzung 	<ul style="list-style-type: none"> Name der Konferenz Einwahlnummer Konferenz-ID Passwort Datum und Uhrzeit von Beginn und Ende der Konferenz Link für Web Collaboration Sitzung 	<ul style="list-style-type: none"> Name der Konferenz Einwahlnummer Konferenz-ID Passwort Link für Web Collaboration Sitzung 	<ul style="list-style-type: none"> Name der Konferenz Einwahlnummer Konferenz-ID Passwort
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
- Zweitanzruf 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.
- 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.

Anmerkung: 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.

Tipp: 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.

12.7.2 Ad-hoc-Konferenz

Eine ad-hoc Konferenz findet spontan statt und wird vom Konferenzleiter manuell gestartet. Der Konferenzleiter kann Ad-hoc-Konferenzen speichern, um sie zu einem beliebigen Zeitpunkt erneut einzuberufen.

Starten 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. Dieses Leistungsmerkmal ist nicht möglich bei CallMe.

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).

Anmerkung: 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 konfigurierbarem Verbindungsaufbau ruft das System die Konferenzteilnehmer an oder diese können sich selbst einwählen. Das System kündigt jeden hinzukommenden Teilnehmer mittels Ansage namentlich an: "... nimmt an der Konferenz teil.", vorausgesetzt der Initiator hat seine Namensansage aufgezeichnet.

Anmerkung: 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.

Anmerkung: Mobility-Entry-Teilnehmer müssen vor ihrer Authentifizierung die Kennzahl für DTMF-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 xA0;for xA0;Desktop oder myPortal xA0;for xA0;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 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.

Die automatische Aufzeichnung einer permanenten Konferenz beginnt dann, wenn zwei oder mehrere Teilnehmer vorhanden sind und hört wieder auf, wenn weniger als zwei Teilnehmer vorhanden sind. Nach der Aufzeichnung erhalten alle Teilnehmer dieselbe Aufzeichnungsdatei der gesamten Konferenz.

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.

Anmerkung: 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: "... 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.

12.8 Web Collaboration

Die UC PC Clients myPortal for Desktop (Windows) und myPortal for Outlook unterstützen innerhalb von Telefongesprächen und Konferenzen die komfortable Einbindung des separaten Produktes Web Collaboration für die gleichzeitige multimediale Zusammenarbeit. Diese bietet schnellen Zugriff auf Funktionen wie Desktop- und Anwendungsfreigabe, Dateifreigabe, Co-Browsing, Whiteboarding, URL-Push, IM-Chat und Video-Chat mit mehreren Teilnehmern.

Die Web Collaboration kann von einem Teilnehmer während eines Telefongesprächs über das Popup-Fenster des UC PC Clients oder innerhalb einer aktiven Konferenz vom Konferenzleiter gestartet werden. Dabei öffnet sich die Web Collaboration Sitzung. Eine lokale Installation von Web Collaboration auf dem UC PC Client ist nicht erforderlich. Ist auf dem UC PC Client ein E-Mail-Programm hinterlegt, kann den Gesprächsteilnehmern eine E-Mail mit dem Link auf den Web Collaboration Client zugesendet werden. Informationen zu Web Collaboration finden Sie in der Web Collaboration Produktdokumentation.

Beim Anlegen oder Bearbeiten einer Konferenz kann der Konferenzleiter eine Web Collaboration Sitzung mit einplanen. Beim Löschen oder Beenden einer Konferenz wird die zugehörige Web Collaboration Sitzung automatisch gelöscht.

Anmerkung: Damit UC PC Clients Web Collaboration automatisch starten können, muss beim Internetzugang der UC PC Clients über einen Proxy-Server die Proxy-Authentifizierung deaktiviert sein.

Unterstützte Arten von Verbindungen

Die Web Collaboration-Einbindung unterstützt Telefongespräche, telefontesteuerte Konferenzen sowie folgende Arten von applikationsgesteuerten Konferenzen:

- Ad-hoc-Konferenz
- Geplante Konferenz
- Permanente Konferenz

Einbindung von Web Collaboration

Für die Einbindung von 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.

Anmerkung: Für die Nutzung von Web Collaboration benötigt das Kommunikationssystem eine Internet-Verbindung (Default Router und DNS-Server). Verbindungen über Proxy werden nicht unterstützt.

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.

Anmerkung: 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.

Instant Messaging und Web Collaboration

Instant Messaging des Systems und Instant Messaging von Web Collaboration sind voneinander unabhängig: Sofortnachrichten aus einem UC PC Client erscheinen nicht in einer Web Collaboration Sitzung des selben Teilnehmers und umgekehrt.

12.9 Instant Messaging

Instant Messaging ist die Kommunikation mittels Sofortnachrichten (Chat).

12.9.1 Sofortnachricht versenden

Mittels Sofortnachrichten können Sie mit anderen Kommunikationspartnern chatten. Das System unterstützt sowohl Benutzer von UC Smart als auch einen externen

Kommunikationspartner 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 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 hier maximal einen externen Kommunikationspartner.

Instant Messaging und Web Collaboration

Instant Messaging des Systems und Instant Messaging einer Web Collaboration-Sitzung sind voneinander unabhängig: Sofortnachrichten aus einem UC PC-Client erscheinen nicht in einer Web Collaboration-Sitzung desselben Teilnehmers und umgekehrt.

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.

12.11 Sprach- und Faxnachrichten

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.

12.11.1 Voicemail-Postfach

Die Sprachbox zeichnet zentral Sprachnachrichten und mitgeschnittene Gespräche auf. Teilnehmer können darauf telefonisch sowie mit UC Smart Clients zugreifen.

Anmerkung: Das voreingestellte Sprachbox-Passwort kann nur über eine interne Rufnummer geändert werden.

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** lautet
- über ein beliebiges externes Telefon

Mit myAttendant kann der Vermittler auch Sprachnachrichten anderer Teilnehmer abhören, die dies ausdrücklich erlaubt haben.

Der Teilnehmer verwaltet die eingegangenen Sprachnachrichten über Ordner wie Posteingang, Abgespielt, Gespeichert oder Gelöscht.

Sprachnachrichten können auch wiedergegeben, angehalten und an einen anderen Teilnehmer weitergeleitet werden. Zusätzlich kann der Teilnehmer Sprachnachrichten im .wav-Format abspeichern und an eine beliebige ausgewählte E-Mail-Adresse weiterleiten.

Über die Sprachbox verwaltet der Teilnehmer auch aufgezeichnete (mitgeschnittene) Gespräche. Aufgezeichnete Gespräche werden in der Sprachbox mit einem entsprechenden Symbol gekennzeichnet.

Anmerkung: 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 ihre Sprachnachrichten als normal, dringend oder vertraulich markieren.

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, wie viele Nachrichten dringend, vertraulich bzw. normal sind. Dringende 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 Umfang der Sprachbox festlegen. Er kann wählen zwischen:

- **Voll**
Voller Funktionsumfang der 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.

Neue Nachrichten auf dem Telefon anzeigen

Sprachnachrichten werden am Telefon angezeigt. Sobald die Sprachnachricht abgespielt wurde, werden die Anzeigen gelöscht.

Die Art der Signalisierung neuer Sprachnachrichten ist endgerätespezifisch

- Für alle Telefone 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.

Benachrichtigungsdienst

Über myPortal oder myPortal for Desktop 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

Themenbereich	Abhängigkeit
Nachricht über Telefon wiedergeben	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.

12.11.2 Ansagen der Sprachbox

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.

Anmerkung: 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 gesetzten 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 Sick Pause Außer Haus ...
Sprachbox mit Anwesenheitsstatus	Standardbegrüßung + Anrufermenü	Name + Anwesenheitsstatus + Anrufermenü
Sprachbox bei gesperrtem Anwesenheitsstatus	Standardbegrüßung + Anrufermenü (wenn aktiviert)	

	Besetzt Nicht angenommen Anrufschutz	Besprechung Sick Pause Außer Haus ...
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 übermittelt 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.

12.11.3 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 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.

Anmerkung: Um eine TIFF-Datei in eine PDF-Datei zu konvertieren, muss die Seite im Format A4 vorliegen.

Aufbewahrungsdauer für Faxnachrichten

Das System löscht automatisch Faxnachrichten, deren Alter folgende Aufbewahrungsdauer überschreitet:

Faxnachricht	Aufbewahrungsdauer (Tage)
Neu	120
Gelesen	365
Gesendet	365
Gelöscht	60

12.11.4 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 Pop-up-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 nur Zeichen des ANSI-Zeichensatzes enthalten. Anders gesagt, es dürfen keine Sonderzeichen oder Umlaute verwendet werden. Da die Kopfzeile grundsätzlich den Namen des Absenders enthalten kann, dürfen die Namen der Teilnehmer keine Sonderzeichen oder Umlaute enthalten.

12.11.5 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:

Benachrichtigung	für Sprachnachricht	für Faxnachricht	Voraussetzungen
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 (Durchschnitt: 1 MB/Min.) 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.

12.11.6 E-Mail-Versand

E-Mail-Versand ermöglicht die Benachrichtigung von Teilnehmern bei neuen Sprach- und Faxnachrichten sowie des Administrators bei Systemmeldungen.

12.11.7 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.

Anmerkung: 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.

12.11.8 Fax over IP (T.38 / G.711-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 Business 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- oder G.711-Faxverbindungen.

Anmerkung: Sofern möglich wird die Verwendung von T.38-Fax empfohlen.

Das System unterstützt für T.38 oder G.711 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.

Anmerkung: Für die Faxbox ist im System T.38 zu aktivieren. Bei Faxversand vom Kommunikationssystem über einen ITSP muss dieser T.38 unterstützen. Wenn der ITSP T.38 nicht unterstützt, wird das Fax als G.711 behandelt.

12.12 Überblick über Integration von Microsoft Office 365

Sie können problemlos zusammenarbeiten und haben überall Zugriff auf E-Mails, Webkonferenzen, Dokumente und Kalender. Das Paket bietet Sicherheit auf Unternehmensniveau und wird von Microsoft unterstützt. Egal, ob Sie ein kleines Unternehmen oder ein multinationales Unternehmen sind, Office 365 bietet Pläne, die auf die individuellen Bedürfnisse Ihres Unternehmens zugeschnitten sind. Für weitere Informationen oder ein 30-Tage-Konto besuchen Sie bitte

OpenScape Business mit Microsoft Office 365

Wenn ein Benutzer einen Termin in seinem Microsoft Outlook-Kalender einstellt, sucht das OpenScape Business-System automatisch nach Schlüsselwörtern in den Betreffs des Termins, zum Beispiel: "Besprechung", "krank", "Pause", "außer Haus". Wenn ein solches Schlüsselwort gefunden wird, setzt das System den Anwesenheitsstatus des Benutzers automatisch, wenn der Termin erreicht ist, auch wenn die Microsoft Outlook-Sitzung dieses Benutzers nicht mehr aktiv ist.

Der Benutzer konfiguriert die Termine mit diesen Schlüsselwörtern und OpenScape Business setzt automatisch den Telefonpräsenzstatus des Benutzers und leitet die Anrufe je nach Einstellung an die Voicemail oder z. B. an das Mobiltelefon weiter. Der Benutzer kann auch in einem allgemeinen Kundenstatus konfigurieren, ob der Anwesenheitsstatus nach Beendigung des Termins wieder in den Büro-Anwesenheitsstatus wechseln soll.

Dies funktioniert auch dann, wenn der Benutzer nicht den lokalen Outlook-Client verwendet und einen Termin mit den oben genannten Schlüsselwörtern direkt auf der Outlook-Webseite in der Cloud einrichtet.

E-Mail-Weiterleitung:

OpenScape Business ist in der Lage, E-Mails an Microsoft Office 365 inklusive Microsoft Exchange Server zu senden.

Dies ermöglicht es den Benutzern, E-Mails für neue Voicemails, Faxe oder Telefonkonferenzen zu erhalten und automatisch Web-Collaboration-Sitzungen von OpenScape Business aus durchzuführen.

OpenScape Business generiert für solche Aktionen E-Mails und hält die Benutzer auch per E-Mail auf dem Laufenden, wenn eine solche neue Benachrichtigung im OpenScape Business-Nachrichtenfeld eintrifft.

13 Funktionen am Telefon

Das Kommunikationssystem bietet vielfältige Telefonie-Leistungsmerkmale, angefangen bei z.B. Halten, Makeln und Rückfrage, über unterschiedliche Anrufsignalisierungen bis hin zu Rufweitschaltung 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.

Anmerkung: 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.

Tipp: Editieren der Wahl ist für jeden Teilnehmer einzeln aktivierbar.

Abhängigkeiten

Thema	Abhängigkeit
Anklopfen	Anklopfen während des Editierens ist möglich, da sich das Telefon im Wahlaufnahmestatus befindet und damit für kommenden Verkehr belegt ist.
Rückfrage	Nach einer Rückfrage befindet sich das Telefon im Wahlaufnahmestatus. Das Editieren von Rufnummernziffern ist damit möglich.

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 anschließende Wahlwiederholung nutzen um dieselbe Nummer erneut zu wählen.

Kurzwahlnummern werden ebenfalls in den Wahlwiederholungsspeicher geschrieben.

Die Wahl interner Rufnummern 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.

13.1.7 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 KWZs 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 aber nur ein KWZ-Bereich zugewiesen werden.

Einträge in Kurzwahllisten können nach Vor- und Nachnamen durchsucht werden, wenn der Name im Format „<Nachname>, <Vorname>“ oder <Vorname>, „<Nachname>“ konfiguriert ist.

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.

Die Zielwahltaste für den Kunden muss wie folgt festgelegt werden:
<Rufnummer><dtmf-Ziffer><Pause-Ziffer><Zugangscode> z.B.
008007728477#P2210344

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

Die Nachwahl wird bei der blockweisen Wahlaussendung (z.B. bei einer ITSP-Konfiguration) nicht unterstützt. Für die "Ziffer für Ziffer"-Ziffern-Übertragung wird sie unterstützt.

Anmerkung:

Das Ziffernübertragungsfeld kann im WBM über den **Expertenmodus > Trunks/Routing > Route** geändert werden

Es besteht die Möglichkeit einer Nachwahl:

- Manuelle Nachwahl

Nach Wahl des Zugangscode 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 zwei 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.

Zum Beispiel: SSD = 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 Kurzwahlruffnummern

Sie können Kurzwahlnummernlisten aus einer XML-Datei im UTF-8-Format importieren. Bereits bestehende Kurzwahlnummern werden vor dem Import gelöscht.

Eine XML-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.

Anmerkung: Der Import von Kurzwahllisten aus CSV-Dateien wird nicht mehr empfohlen und nur noch in Sonderfällen unterstützt.

Export von Kurzwahlruffnummern

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.

13.1.8 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 übernommen 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.

Zugehörige Konzepte

[Teamschaltung / Team-Gruppe](#) auf Seite 382

[Chef/Sekretär / Top-Gruppe](#) auf Seite 386

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.

Funktionen am Telefon

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.

13.1.11 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.

Anmerkung: Bei S₀-Telefonen Leistung vormerken nicht möglich.

13.1.13 Privatleitung

Einer Privatleitung ist eine Amtsleitung, die ausschließlich einem bestimmten Teilnehmer zur Verfügung steht.

Funktionen am Telefon

Anrufsignalisierung, Rufnummernanzeige

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 Calling Line Identification Presentation (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

13.2.3 Calling Line Identification Restriction (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.

Tipp: 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.

13.2.4 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.

13.2.5 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 Ortsnetzkenzahl, mit Ortsnetzkenzahl (national) oder zusätzlich die internationale Länderkenzahl (international) enthält.

Tipp: CLIP no screening muss vom Netzanbieter unterstützt werden und aktiviert sein.

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.

Tipp: 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.

Funktionen am Telefon

Funktionen während der Verbindung

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.

Anmerkung: Detaillierte Anweisungen zum Parken von Anrufen und zur Wiederaufnahme von geparkten Anrufen finden Sie im entsprechenden Kapitel der Bedienungsanleitung des jeweiligen Geräts (OpenStage X / HiPath/OpenScape 3000/4000 Bedienungsanleitung).

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 Supervision

Call Supervision 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.

Die Funktion ist in der Standardkonfiguration deaktiviert. Sie kann nur aktiviert werden, wenn die landesspezifische Gesetzgebung dies zulässt. Im Einzelfall muss die landesspezifische Gesetzgebung immer geprüft werden, bevor die Funktion aktiviert wird.

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 der Call Supervision 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

Themenbereich	Abhängigkeit
Schnurlose Telefone	Sie können Call Supervision nicht an einem schnurlosen Telefon verwenden, da dieses die automatische Mikrofon-Stummschaltung nicht unterstützt.
Konferenzschaltung	Call Supervision schränkt die mögliche Anzahl an Konferenzen ein. Maximale Anzahl möglicher Konferenzen im System = maximale Anzahl gleichzeitiger Call-Supervision-Teilnehmer.
Call Supervision	Der Anruf kann nur mithilfe des Codes *944 + Rufnummer aufgeschaltet werden (nicht über ein Menü).
Call Supervision	Um die Verwendung von Funktionen für einen Teilnehmer zu ermöglichen, müssen das Teilnehmer-Flag Call Supervision und das Flag Aufschaltberechtigung ein aktiviert werden. (Funktion kann nicht mit CSTA-Monitoring verwendet werden.)

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.

Anmerkung: 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.

Anmerkung: 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.

Anmerkung: Wenn Diskretes Ansprechen aktiviert ist, sind die Leistungsmerkmale Anruf weiterleiten/übergeben und Konferenz in UC Suite-Produkten nicht verfügbar.

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:

Funktionen am Telefon

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
Übergabe	--	--	--	--	--	--
Konferenz	--	--	--	--	--	--
Anklopfen	Ja	--	Ja	--	Ja	--
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	--	--	--	--	--	--

13.3.9 Live Call Recording (Voice Recording; Sprachaufzeichnung)

Das Leistungsmerkmal ermöglicht die Aufzeichnung der Daten einer aktiven Sprachverbindung zwischen zwei Teilnehmern (ein Teilnehmer muss intern, der andere kann ein externer Teilnehmer sein), also der Aufnahme von Gesprächen. Für die Aufzeichnung ist ein separates Gerät erforderlich.

Der Start/Stop der Aufzeichnung kann per Funktionstaste oder Kennzahl (analoge Endgeräte) erfolgen. In Abhängigkeit von der Konfiguration kann die Aufzeichnung auch durch das Aufzeichnungsgerät angehalten werden.

Die Aufzeichnungsvorrichtung kann von allen unterstützten Endgeräten innerhalb einer CorNet-NQ-Vernetzung genutzt werden. Nicht unterstützt werden Verbindungen mit CorNet N und QSIG (ECMA, ISO). Der Aufzeichnungston während der Aufnahme kann abgeschaltet werden.

Unterstützt werden TDM- und CorNet-IP (HFA)-Telefone (inkl. Geräte ohne Display) sowie auch OpenScape Personal Edition (HFA) und optiClient Attendant. Nicht unterstützt werden Standard H.323-Telefone, SIP-Telefone, EDSS1-Teilnehmer.

Anmerkung: Ein aktivierte Anrufaufnahme wird durch eine LED bzw. durch einen Aufzeichnungston während des Gesprächs angezeigt.

Es kann für jeden Teilnehmer einzeln konfiguriert werden, ob er Voice Recording nutzen darf.

Abhängigkeiten/Einschränkungen

Thema	Abhängigkeit/Einschränkung
Rückfrage, Makeln, Transfer, Konferenz	Wenn Sie während einer Anrufaufzeichnung eines dieser Leistungsmerkmale einleiten, so wird die Aufzeichnung des Gesprächs automatisch abgebrochen.
Halten	Bei Aktivierung von "Halten" wird eine laufende Aufzeichnung abgebrochen. Eine Aktivierung der Aufzeichnung ist nicht möglich, wenn man einen Teilnehmer gehalten hat.
Aufschalten	Anrufaufzeichnung nicht möglich. Man kann sich auf ein Gespräch, welches aufgezeichnet wird, nicht aufschalten. Ebenso ist es nicht möglich nach dem Aufschalten eine Aufzeichnung zu aktivieren.
Call Supervision	Anrufaufzeichnung nicht möglich. Man kann ein Gespräch, welches aufgezeichnet wird, nicht mithören. Ebenso ist es nicht möglich nach der Aktivierung von „Call Supervision“ eine Aufzeichnung zu starten.

Anmerkung: Es können nur Zweier-Gespräche aufgezeichnet werden, keine Konferenzen oder Gespräche, bei denen zusätzlich ein gehaltener Teilnehmer beteiligt ist.

Anmerkung: Zusätzliche Hinweise:

-) Das Aufzeichnungsgerät kann in einem beliebigen Knoten eines Cornet-NQ-Netzes adressiert werden.
-) Es kann nur einer beschränkten Anzahl von Teilnehmern in einem Knoten die Berechtigung für Gesprächsaufzeichnung erteilt werden (derzeit: 50).
-) Während der Aufzeichnung werden Konferenz-Ressourcen belegt.

-) Die Standard-Service-Kennzahl zur Aktivierung der Gesprächsaufzeichnung lautet *493.

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 Anrufumleitung

Die Rufweiserschaltung leitet Anrufe weiter, wenn sie nicht innerhalb einer bestimmten Zeit angenommen werden.

Diese Art der Rufweiserschaltung wird auch als Feste Rufweiserschaltung bezeichnet, weil Sie nur durch den Administrator konfigurierbar ist.

Für jede Rufweiserschaltung 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 Rufweiserschaltungsziel 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.

Rufweiserschaltung im Besetztfall

Die Rufweiserschaltung 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 Rufweiserschaltung eingerichtet, wird der Anruf nicht weitergeschaltet.

Abhängigkeiten

Themenbereich	Abhängigkeit
Analoge Telefone	Bei diesen Telefonen ist nicht zu erkennen, dass es sich bei dem eingehenden Ruf um einen weitergeleiteten Ruf handelt.
Anklopfen annehmen	Hat ein Teilnehmer Anklopfen freigegeben, wird bei ihm auch dann angeklopft, wenn für ihn Rufweilerschaltung im Besetztfall konfiguriert ist.
Anrufschutz	Ein Rufziel, das den Anklopfschutz aktiviert hat, wird übersprungen.
Anrufumleitung	Eine Rufweilerschaltung wird erst ausgeführt, wenn nach einer vom Administrator eingestellten Zeit das Ziel einer Anrufumleitung nicht antwortet.
Nachtschaltung	Wird für einen Teilnehmer in der Rufweilerschaltung 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".
Rufweilerschaltung ins Amt	Ist eine Rufweilerschaltung ins Amt aktiviert, so hat diese Vorrang vor anderen Rufweilerschaltungen.
Sammelanschluss / Gruppenruf	<p>Wird eine Gruppe oder ein Sammelanschluss als Ziel einer Rufweilerschaltung eingetragen, so wird diese Gruppe erst vollständig abgearbeitet, d.h. nacheinander gerufen, bevor das nächste Ziel der Rufweilerschaltung ausgewertet wird. Gruppenruf und Sammelanschluss sind wie eine Rufweilerschaltung innerhalb der Rufweilerschaltung anzusehen.</p> <p>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.</p>

13.4.2 Anrufumleitung (CF)

Mit der Anrufumleitung (AUL) können Teilnehmer kommende 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:

Funktionen am Telefon

- All Anrufe
- Nur externe Anrufe
- Nur interne Anrufe

Folgende Ziele für eine Anrufumleitung sind möglich:

- Anderes Telefon (intern oder extern)
- Vermittlungsplatz
- Sprachbox
- Gruppennummer
- 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 Rufweitschaltung bei diesem Ziel. Eventuell eingetragenen weiteren Ziele in der Rufzielliste wird nicht gefolgt.

Soll eine Rufweitschaltung zu weiteren Zielen erfolgen, muss das Systemflag **Rufweitschaltung 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** aktivieren.

Anmerkung: Wenn ein Anruf über Smart AA geleitet wird und dieser Anruf an einen Benutzer A weitergeleitet wird, wobei die externe Weiterleitung (*11) an Benutzer B aktiviert ist, wird Benutzer B nicht die CLI des Anrufers, sondern die Durchwahl des Benutzers A angezeigt.

Abhängigkeiten

Themenbereich	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.

Themenbereich	Abhängigkeit
UCD-Gruppe als Anrufumleitungsziel	<p>In folgenden Fällen wird der Anrufumleitung zu einer UCD-Gruppe nicht gefolgt:</p> <ul style="list-style-type: none"> • 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 AUL wird gefolgt.

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 Rufweitschaltung 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 eingetragen werden.

Das Umleitungsziel wird nicht dauerhaft gespeichert und bei Deaktivierung des Leistungsmerkmals gelöscht.

Im Besetztfall gelten die Regeln der Rufweitschaltung, 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 Rufweiserschaltung im Amt (nicht für USA)

Jeder Teilnehmer, dem als Durchwahlrufnummer eine MSN (Multiple Subscriber Number beim ISDN-Mehrgeräteanschluss oder ITSP-Anschluss) zugeordnet ist, kann für diese MSN eine Rufweiserschaltung im Amt aktivieren bzw. deaktivieren. Voraussetzung ist, dass der Teilnehmer die Berechtigung für externe Rufweiserschaltung hat.

Ist einer Teilnehmergruppe eine MSN zugeordnet, kann jeder Teilnehmer dieser Gruppe für diese MSN eine Rufweiserschaltung im Amt aktivieren bzw. deaktivieren.

Das Leistungsmerkmal wird in drei Varianten unterschieden:

- Uneingeschränkte Gesprächsumleitung (CFU): Der Netzanbieter leitet alle für diese MSN bestimmten Rufe direkt weiter, unabhängig von deren Status.
- Anrufumleitung bei Besetzt (CFB = Call Forwarding Busy): Die Rufweiserschaltung wird nur ausgeführt, wenn die gewählte MSN besetzt ist.
- Verzögerte Anrufumleitung (CFNR = Call Forwarding No Reply): Die Rufweiserschaltung wird nur ausgeführt, wenn der eingehende Ruf nicht innerhalb einer vorgegebenen Zeit beantwortet wird.

Anmerkung:

Anmerkung: Für alle oben genannten Szenarien der Anrufumleitung kann der Benutzer nur ein Weiserschaltungsziel pro MSN eingeben. Die maximale Anzahl weiserschaltbarer MSN ist 10.

Falls ITSP oder ISDN mit der Durchwahl konfiguriert ist, sind maximal 249 externe Umleitungen möglich.

Abhängigkeiten

Themenbereich	Abhängigkeit
Nachtschaltung	Rufweiserschaltung im Amt hat höhere Priorität als Nachtschaltung.

13.4.5 Rufzuordnung

Die Rufzuordnung ermöglicht eine Rufweiserschaltung von ankommenden Anrufen einer analogen oder S₀-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.

13.4.6 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" (= rufzuschaltender 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 Anrufe abweisen

Kommende interne und externe Erstanrufe kann der Teilnehmer abweisen. Die Anrufe können durch Betätigen der Trenntaste abgewiesen werden.

Der abgewiesene Anruf folgt anschließend der Rufweitzuschaltung. Ist kein Rufweitzuschaltungsziel 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, weitergeleitete Anrufe, vorgemerkte Rückrufe, gehaltene oder geparkte Gespräche können nicht abgewiesen werden. Wird ein Gespräch zum Abwurfplatz abgeworfen, kann es nicht abgewiesen werden.

Abhängigkeiten

Themenbereich	Abhängigkeit
Gruppenruf, Sammelruf, MULAP	In diesen Fällen wird der gesamte Gruppenanruf beendet und der Anruf folgt der konfigurierten Rufweitzuschaltung. 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 anrufgeschützten 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.
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 annimmt, 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 Rufweilerschaltung im Besetztfall konfiguriert ist.

Anklopfen freigeben

Anklopfen durch den Vermittlungsplatz

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 Rufweilerschaltung im Besetztfall konfiguriert hat.

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.

Thema	Abhängigkeit
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.

13.5.3 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.

Thema	Abhängigkeit
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.

13.5.4 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.

13.5.5 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.

Anmerkung: Der Empfang von Message Waiting Indication (MWI)-Meldungen ist auf 100 Telefone beschränkt; bei weiteren Telefonen schlägt der Empfang fehl.

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.

13.5.6 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 Leistungsmerkmals

Bevor ein Teilnehmer Assoziierte Dienste benutzen kann, muss er das Codeschloss des anderen Teilnehmers deaktivieren, falls aktiviert.

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 zuruecksetzen	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 Sicherheits-Modus für DISA.

Für eine weitere Aktion über DISA muss sich der Teilnehmer erneut anmelden.

Anmerkung: Wenn in OpenScape Business X eine DISA-Rufnummer angerufen wird, hören Sie einen Dauerton. Wenn in OpenScape Business S eine DISA-Rufnummer angerufen wird, hören Sie Wartemusik.

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 Telefentypen benutzen. Relocate ermöglicht 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 Telefentyps, d.h. mit identischem Tastenlayout getauscht werden. Beim Tausch von Benutzerprofilen unterschiedlicher Telefentypen 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.

13.5.10 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	Wahlbereich		Im Gespräch	Gehend	Kommender Ruf
	Besetzt	Frei			
Anrufübernahme, gezielt	x	-	x	-	-
Anrufumleitung ein (nicht bei Gemeinschaftsanlagen; nicht für einzelne MSN eines S ₀ -Amtsanschlusses)	x	-	x	x	-

Funktionen am Telefon

Leistungsmerkmal	Wahlberechtigt	Besetzt	Im Gespräch		
			Gehend	Ruf	Kommender Ruf
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	-
Info senden (Message Waiting)	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	-
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.

13.6 Übersicht über Funktionen und Codes

Servicekennzahl	Beschreibung
*0	Zurück zum Wartenden
*1	Anrufumleitung
*2	Makeln
*3	Konferenz
*44	Nachtschaltung ein
*51	Flash zum Amt
*52	Mute ein
*53	DTMF-Wahl
*55	Anklopfen annehmen
*56	Parken einleiten
*57	Anrufübernahme in AUN-Gruppen
*58	Rückruf einleiten
*59	Anrufübernahme ausserhalb AUN-Gruppen
*60	Projektkennzahl
*61	Türöffner

Funktionen am Telefon

Servicekennzahl	Beschreibung
*62	Aufschalten
*64	Anrufumleitung im Amt (ISDN) ein
*65	Kosten abfragen
*66	Codeschloss ein
*67	Assoziierte Wahl
*68	Info senden
*69	Abwesenheitstext ein
*7	KWZ/KWI ausspeichern
*80	Direktansprechen
*90	Einstieg zur Aktivierung der Aktoren (einschalten)
*91	Tastenprogrammierung
*92	Kurzrufnummer ändern
*93	PIN ändern
*940	Endgerätetest
*95	Systemverwaltung
*97	Anrufschutz DND ein
	Babyphone ein
*81	Rufzuschaltung ein
#1	Anrufumleitung aus
#44	Nachtschaltung aus
#52	Mute aus
#56	Zurück zum Wartenden
#58	Rückrufe abfragen/löschen
#64	Anrufumleitung im Amt (ISDN) aus
#66	Codeschloss aus
#68	Info (gesendete) lesen/löschen
#69	Abwesenheitstext aus
#97	Anrufschutz DND aus
*96	Direktantworten ein
#96	Direktantworten aus
#90	Einstieg zur Deaktivierung der Aktoren (ausschalten)
#81	Rufzuschaltung aus
#0	Alle Dienste zurücksetzen

Servicekennzahl	Beschreibung
#3	Fünferkonferenz aus
#82	Anruferliste abfragen
*83	Assoziierte Dienste
*84	Fangen
*85	Gruppenruf ein
#85	Gruppenruf aus
*82	Anruferliste beschreiben
*86	Rufnummerunterdrückung ein
#86	Rufnummerunterdrückung aus
*87	Stilles Anklopfen ein
#87	Stilles Anklopfen aus
*98	Ruhe ein
#98	Ruhe aus
*991	remote DTMF-Systemverwaltung
*992	remote DTMF-Systemverwaltung freigeben
*993	remote ISDN-Systemverwaltung freigeben (überholt)
*994	remote Anlagendaten-Abfrage freigeben (z.Z. inaktiv)
*89	Türöffner via DTMF Code freigeben
#89	Türöffner via DTMF Code sperren
*63	Wiederaufnahme eines externen Gesprächs nach Haltentaste
*41	Rufnummern zuweisen bei MUSAP
*401	UCD-Agenten einloggen
#401	UCD-Agenten ausloggen
*402	UCD-Agent verfügbar
#402	UCD-Agent nicht verfügbar
*403	UCD-Nachbearbeitung ein
#403	UCD-Nachbearbeitung aus
*404	UCD-Nachtschaltung ein
#404	UCD-Nachtschaltung aus
*405	UCD-Rufqueue-Status abfragen
*42	Telephone Data Service (TDS)
*43	Ltg freischalten

Funktionen am Telefon

Servicekennzahl	Beschreibung
*45	PSE: Suchen
#45	PSE: Melden
*46	Weckeinrichtung: Termin ein
#46	Weckeinrichtung: Termin aus
*9419	Endgerätetausch aktivieren
#9419	Endgerätetausch deaktivieren
*942	Anmeldebereitschaft (Mobilteil)
*943	Zentrales Codeschloss
*944	Call Supervision
	Drop Last Conference Party within CO (USA only)
*490	Freigeben zum Anklopfen aktivieren
#490	Freigeben zum Anklopfen deaktivieren
*48	Sprachauswahl
*508	Flex Call
*502	Rufumschaltung für MULAP ein
#502	Rufumschaltung für MULAP aus
*501	AUL für MULAP ein
#501	AUL für MULAP aus
*509	Trace einfrieren
*47	DISA intern
*503	Keypad-Wahl
*54	Internes Telefonbuch
*491	analoges Hotelendgerät
#943	Zentrales Codeschloss / Code rücksetzen
*9411	Rufweitzerschaltung Gerät ausser Betrieb ein
#9411	Rufweitzerschaltung Gerät ausser Betrieb aus
*493	Sprachaufzeichnung ein
#493	Sprachaufzeichnung aus
*495	Umleitung nach Zeit ein
#495	Umleitung nach Zeit aus
*945	Diskretes Ansprechen
*494	Data I/O

Servicekennzahl	Beschreibung
*996	Smart Services via HTTPS für remote Verwaltung freigeben
#996	Smart Services via HTTPS für remote Verwaltung deaktivieren
*997	Kontrolliertes Herunterfahren

Arbeiten im Team (Gruppen)

Anrufübernahmegruppe, Gruppenruf und Sammelanschluss

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.

Tipp: 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.

Anmerkung: Anführungszeichen (") sind für den Namen einer AUN-Gruppe nicht zulässig.

SIP-Telefone

Die Einbindung von SIP-Telefonen in eine Anrufübernahmegruppe ist möglich.

Tipp: 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

Themenbereich	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.

Zugehörige Tasks

[Wie Sie eine Anrufübernahmegruppe 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 Gruppenmitglieder-Telefonen signalisiert. Der zuerst abhebende Teilnehmer wird mit dem Anrufenden verbunden.

Jedes Mitglied eines Gruppenrufs ist auch unter seiner 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 Anklopftton signalisiert. Legt ein Teilnehmer auf, wird der Anruf weiterhin bei allen Gruppenmitgliedern signalisiert (Anklopftton bei besetzten Gruppenmitgliedern).

Sind alle Gruppenmitglieder besetzt und alle haben das Leistungsmerkmal „Anrufschutz“ aktiviert, erhält ein Anrufer den Besetztton. Ist ein Anrufumleitungsziel für diese Gruppe definiert, erhält der Anrufer keinen Besetztton, sondern wird direkt zum nächsten Anrufumleitungsziel weitergeschaltet.

- 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.

Anmerkung: Der Anwesenheitsstatus eines externen Ziels, das zur Gruppe gehört, kann nicht erkannt werden.

- Anklopfen

Incoming calls are simultaneously signaled at all available group members. Verfügbare Gruppenmitglieder sind Teilnehmer, die nicht besetzt sind. Bei besetzten Gruppenmitgliedern wird ein anstehender Anruf sofort durch einen Anklopftton signalisiert.

Voraussetzung dafür ist, dass bei allen Gruppenmitgliedern der Anrufschutz deaktiviert ist.

Gruppenrufe werden von der Anrufumleitung (Nicht angenommen) wie Teilnehmer behandelt. Das heißt, wenn ein Anruf von keinem Mitglied eines Gruppenrufs angenommen werden kann, wird dieser zu einem Anrufumleitungsziel entsprechend der Rufzielliste weitergeschaltet. Dabei kann festgelegt werden, ob eine Anrufumleitung 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 überschreiten.

Im Display eines 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.

Arbeiten im Team (Gruppen)

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 Rufwefterschaltung zur Gruppenruf-Sprachbox. Voraussetzung dafür ist, dass die Gruppenruf-Sprachbox als Anrufumleitung - Anrufwefterschaltung (CFNA) dieses Gruppenrufs definiert wurde.

Nimmt ein Mitglied einen kommenden Anruf an seine eigene Teilnehmerrufnummer nicht an, wird dieser Anruf zu einem Anrufumleitungsziel 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 Anrufumleitung (Nicht angenommen) nach Zeitüberschreitung zur Gruppenruf-Sprachbox eingerichtet. Jedes Mitglied hat eine Anrufumleitung (Nicht angenommen, CFNA) nach Zeitüberschreitung zur eigenen Sprachbox definiert.		
Ankommender Anruf für Mitglied A (200)	Alle Mitglieder sind frei.	Mitglied A nimmt den Anruf nicht an. Es erfolgt eine Anrufumleitung (Nicht angenommen) nach Zeitüberschreitung zur Sprachbox des Mitglieds A.
	Mitglied A hat eine direkte Anrufumleitung (CFU) zur eigenen Sprachbox definiert. Mitglieder B und C sind frei.	Es erfolgt eine sofortige Rufwefterschaltung zur Sprachbox des Mitglieds A.
Ankommender Anruf für den Gruppenruf (404)	All members are free.	Der Anruf wird bei allen Mitgliedern signalisiert. Kein Mitglied nimmt den Anruf an. Es erfolgt eine Anrufumleitung (Nicht angenommen) nach Zeitüberschreitung zur Gruppenruf-Sprachbox.

	Member A has defined Call Forwarding Unconditional (CFU) to his or her own voicemail box. Members B and C are free.	Der Anruf wird bei den Mitgliedern B und C signalisiert. Kein Mitglied nimmt den Anruf an. Call Forwarding-No Answer after Timeout occurs to the voicemail box of the group call.
	Mitglied A hat eine direkte Anrufumleitung (CFU) zu einem externen Ziel definiert. Members B and C are free.	Der Anruf wird bei den Mitgliedern B und C sowie beim externen Ziel signalisiert. No member accepts the call. Call Forwarding-No Answer after Timeout occurs to the voicemail box of the group call.
	Mitglied A hat über den AutoAttendant Regeln für Anrufumleitung (Nicht ankommend, CFNA) definiert. Members B and C are free.	The call is signaled at all other members. No member accepts the call. Call Forwarding-No Answer after Timeout occurs to the voicemail box of the group call.

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 von Teilnehmern 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 Sammelanschlüssen 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. Sie haben folgende Möglichkeiten:

- Doppel-Rufton (Standardeinstellung)

Arbeiten im Team (Gruppen)

- 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.

Tipp: Bei SIP-Telefonen ist keine Programmierung von Funktionstasten möglich. Darüber hinaus können keine Leistungsmerkmale über Kennzahlen aktiviert oder deaktiviert werden. Spezifische Displaymeldungen eines Gruppenrufs werden nicht unterstützt.

Abhängigkeiten

Themenbereich	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 des Mitglieds.
Aufschalten	Sind alle Mitglieder eines Gruppenrufs besetzt, ist kein Aufschalten möglich.
ISDN-Telefone	Die Einbindung von ISDN-Telefonen in einen Gruppenruf ist nicht möglich.

Zugehörige Konzepte

[Internes Verzeichnis](#) auf Seite 253

Zugehörige Tasks

[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 den Anklopferschutz 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 Rufweitschaltung zur Sammelanschluss-Sprachbox. Voraussetzung dafür ist, dass die Sammelanschluss-Sprachbox als Rufweitschaltungsziel dieses Sammelanschlusses definiert wurde.

Nimmt ein Mitglied einen kommenden Anruf an seine eigene Teilnehmerrufnummer nicht an, wird dieser Anruf zu einem Rufweitschaltungsziel entsprechend der Rufzielliste dieses Teilnehmers weitergeschaltet.

<p>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 Rufweitschaltung nach Zeit zur Sammelanschluss-Sprachbox eingerichtet. Jedes Mitglied hat eine Rufweitschaltung nach Zeit zur eigenen Sprachbox definiert.</p>		
Ankommender Anruf für Mitglied A (200)	Alle Mitglieder sind frei.	Mitglied A nimmt den Anruf nicht an. Es erfolgt eine Rufweitschaltung nach Zeit zur Sprachbox des Mitglieds A.
	Mitglied A hat eine sofortige Rufweitschaltung zur eigenen Sprachbox definiert. Mitglieder B und C sind frei.	Es erfolgt eine sofortige Rufweitschaltung 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 Rufweitschaltung nach Zeit zur Sammelanschluss-Sprachbox.
	Mitglied A hat eine sofortige Rufweitschaltung 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 Rufweitschaltung 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. Sie haben die folgenden Möglichkeiten:

- Doppel-Rufton (Standardeinstellung)
- Dreifach-Rufton
- Kurz/Lang/Kurz-Rufton

Bei analogen Telefonen ist ausschließlich die Standardeinstellung möglich. Änderungen haben keine Auswirkung.

Arbeiten im Team (Gruppen)

SIP-Telefone

Die Einbindung von SIP-Telefonen in einen Sammelanschluss ist möglich.

Tipp: 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.

Zugehörige Tasks

[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 eine Anrufübernahmegruppe konfigurieren](#)
- [Wie Sie ein Mitglied zur Anrufübernahmegruppe hinzufügen oder löschen](#)

Mit dem Wizard **Gruppenruf / Sammelanschluss** können Sie Gruppenrufe des Typs Gruppe einrichten. 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](#)

14.1.5 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 den Anklopferschutz für Gruppenmitglied ein- oder ausschalten](#)

14.2 Teamschaltung / Team-Gruppe und Chef/Sekretär / Top-Gruppe

Eine Teamschaltung / Team-Gruppe bietet komfortable Teamfunktionen. 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.

Anmerkung: Beim Erstellen einer MULAP über die Team/Top-Optionen im WBM/Manager E dürfen keine Rufnummern angegeben werden, die mit ** oder *** beginnen.

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 Direktrufftasten 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. Das Folgende gilt für Gruppen des Typs Gruppenruf, Sammelanschluss, Teamschaltung / Team-Gruppe und Chef/ Sekretariat / Top-Gruppe: Die Summe aller Mitgliedschaften des Teilnehmers in diesen Gruppen darf 32 nicht überschreiten.

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 dieser Leitung durch Blinken der MULAP-Taste angezeigt. Durch das Drücken der MULAP-Taste können sie an der Konferenz teilnehmen.

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 ein gehender Ruf über die MULAP-Leitung des Masters. Dem Angerufenen wird die MULAP-Teilnehmernummer 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.

Arbeiten im Team (Gruppen)

- 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 übernommen 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. Sie haben 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 HFA oder UP0-Telefon) 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.

Tipp: Bei SIP-Telefonen ist keine Programmierung von MULAP-Tasten und Direktruf-tasten möglich. Darüber hinaus können keine Leistungsmerkmale über Kennzahlen aktiviert oder deaktiviert werden. Spezifische Displaymeldungen der Teamschaltung/Team-Gruppe werden nicht unterstützt.

Anmerkung: Hochwertige Telefone, wie CP 400/600/600E/700/700X/710, führen eigene Journaleinträge und können mehr Informationen anzeigen. Bei Gruppenkonfigurationen sind sie jedoch auf Systemdaten angewiesen, da die Gruppen auf dem System und nicht auf den Telefonen konfiguriert werden. Daher kann es vorkommen, dass Informationen über Gruppen in Journaleinträgen nicht angezeigt werden, da sie den Einschränkungen und der Konfiguration des Systems folgen.

Abhängigkeiten

Themenbereich	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.
Gruppen-/Sammelanschlüsse	Die Einbindung eines Basic-/Chef-MULAPs in Teamschaltungen/Team-Gruppen ist nicht möglich.

Zugehörige Konzepte

[Direktruf](#) auf Seite 333

Zugehörige Tasks

[Wie Sie eine Teamschaltung / Team-Gruppe hinzufügen](#)

[Wie Sie eine Teamschaltung / Team-Gruppe ändern](#)

[Wie Sie eine Teamschaltung / Team-Gruppe löschen](#)

[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

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.

Tipp: 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.

Tipp: 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. Das Folgende gilt für Gruppen des Typs Gruppenruf, Sammelanschluss, Teamschaltung / Team-Gruppe und Chef/Sekretariat / Top-Gruppe: Die Summe aller Mitgliedschaften des Teilnehmers in diesen Gruppen darf 32 nicht überschreiten.

Jeder Chef/Sekretär-Konfiguration/Top-Gruppe kann ein maximal 16 Zeichen langer Name zugewiesen werden.

Bei der Einrichtung einer Chef/Sekretär-Konfiguration oder 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 die Chef-MULAP-Leitung für einen Ruf ausgewählt. Kommende Rufe über die zugehörige Chef-MULAP-Rufnummer werden standardmäßig ausschließlich optisch signalisiert.

Standardeinstellung: Chef-Funktionen erhalten alle Chefs der Chef/Sekretär-Konfiguration oder 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 dieser Leitung durch Blinken der MULAP-Taste angezeigt. Durch das Drücken der MULAP-Taste können sie an der Konferenz teilnehmen.

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 ein gehender Ruf 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 übernommen 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. Sie haben 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 ein Systemtelefon (zum Beispiel IP-Telefon, HFA oder SIP) als erstes Mitglied der Chef/Sekretär-Konfiguration/Top-Gruppe (Chef 1) 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.

Tipp: 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.

Anmerkung: Hochwertige Telefone, wie das CP600, führen eigene Journaleinträge und können mehr Informationen anzeigen. Bei Gruppenkonfigurationen sind sie jedoch auf Systemdaten angewiesen, da die Gruppen auf dem System und nicht auf den Telefonen

Arbeiten im Team (Gruppen)

konfiguriert werden. Daher kann es vorkommen, dass Informationen über Gruppen in Journaleinträgen nicht angezeigt werden, da sie den Einschränkungen und der Konfiguration des Systems folgen.

Abhängigkeiten

Themenbereich	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.
Gruppen-/Sammelanschlüsse	Die Einbindung eines Basic-/Chef-MULAPs in Chef/Sekretär-Konfigurationen/Top-Gruppen ist nicht möglich.

Zugehörige Konzepte

[Direktruf](#) auf Seite 333

Zugehörige Tasks

[Wie Sie eine Chef/Sekretär- / Top-Gruppe hinzufügen](#)

[Wie Sie eine Chef/Sekretär- / Top-Gruppe ändern](#)

[Wie Sie eine Chef/Sekretär- / Top-Gruppe löschen](#)

[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](#)

14.2.3 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](#)

Zugehörige Konzepte

[Konfiguration von myPortal to go und Mobility Entry](#) auf Seite 541

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](#)

14.3 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 Ausgangsbelegung ist allen Mastern zugeordnet.

- **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.

Anzeige Nummer / Name

Beim Aufbau eines gehenden Gesprächs wird eine Rufnummer zugewiesen (eigene Rufnummer oder MULAP-Gruppenrufnummer).

Kommend wird beim Melden auf einen ankommenden MULAP-Anruf die MULAP-Gruppenrufnummer zugewiesen.

Bei Anrufen zu einer MULAP

- wird dem Anrufer vor dem Melden der gerufene MULAP-Name und/oder die MULAP-Rufnummer angezeigt.
- wird dem Anrufer nach dem Melden der meldende Teilnehmer-Name und/oder die MULAP-Rufnummer angezeigt.
- Bei Anrufen von einem MULAP-Teilnehmer (MULAP-Taste/Präferenz) wird dem Angerufenen und dem Meldenden immer der Teilnehmer-Name und/oder die MULAP-Rufnummer angezeigt.
- Bei gehender Belegung gilt generell: Führt ein Teilnehmer ein Gespräch auf der eigenen Rufnummer und ist die gehende Präferenz ungleich der eigenen Rufnummer, wird dem Partner immer die Rufnummer der gehende Präferenz angezeigt.

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. Sie haben folgende Möglichkeiten:

- Doppel-Rufton (Standardeinstellung)
- Dreifach-Rufton
- Kurz/Lang/Kurz-Rufton

Arbeiten im Team (Gruppen)

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. Als Voraussetzung muss ein TDM-, HFA- oder SIP-Telefon als erstes Mitglied des Basic MULAP definiert sein.

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.

Tipp: 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

Themenbereich	Abhängigkeit
Anrufschutz	Nach Aktivierung des Anrufschutzes, werden ankommende Anrufe nicht durchgestellt.
ISDN-Telefone	Die Einbindung von ISDN-Telefonen in Basic-MULAPs ist nicht möglich.

Zugehörige Tasks

[Basic-MULAP hinzufügen](#)

[Wie Sie Basic-MULAP anzeigen oder ändern](#)

[Wie Sie eine 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 sowie unter ihren eigenen Teilnehmerrufnummern erreichbar.

Tipp: 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 dieser Leitung durch Blinken

der MULAP-Taste angezeigt. Durch das Drücken der MULAP-Taste können sie an der Konferenz teilnehmen.

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 ein gehender Ruf 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. Sie haben 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 ein Systemtelefon (z. B. HFA oder UP0-Telefon) als erstes Mitglied der Chef-MULAP (Chef 1) 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.

Tipp: 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

Themenbereich	Abhängigkeit
Anrufschutz	Nach Aktivierung des Anrufschutzes, werden ankommende Anrufe nicht durchgestellt.
ISDN-Telefone	Die Einbindung von ISDN-Telefonen in Chef-MULAPs ist nicht möglich.

Zugehörige Tasks

[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 eine Basic-MULAP hinzufügen](#)
- [Wie Sie Basic-MULAP anzeigen oder ändern](#)
- [Wie Sie eine 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](#)

14.4 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 <i>Rufzuschaltung</i> ist nicht möglich.

Zugehörige Tasks

[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.

Zugehörige Tasks

[Faxbox-Gruppe konfigurieren](#)

[Wie Sie eine Faxbox-Gruppe anzeigen oder ändern](#)

[Mitglied zur Faxbox-Gruppe hinzufügen oder löschen](#)

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](#)

14.5 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

Arbeiten im Team (Gruppen)

Anrufverteilung (UCD Uniform Call Distribution)

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 festgelegt 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

Arbeiten im Team (Gruppen)

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	<p>In folgenden Fällen wird der Anrufumleitung zu einer UCD-Gruppe nicht gefolgt:</p> <ul style="list-style-type: none">• 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.

14.6.2 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).
Nachbearbeitung	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 Rufwefterschaltung 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.

14.6.3 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.

14.6.4 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.

14.6.5 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.

14.6.6 UCD-Warteschlange

Sind alle Agenten einer UCD-Gruppe belegt, können kommende Anrufe in eine Warteschlange eingetragen werden. Wartenden Anrufern können Ansagen oder Musik eingespielt werden.

Arbeiten im Team (Gruppen)

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 festgelegt 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.

14.6.7 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.

Anmerkung: Beim UCD-Überlauf-Konzept wird nur ein Überlauf-Ziel definiert (zweiter CDL-Eintrag). Daher werden Ansagen erst dann wiedergegeben, wenn der Anruf beim UCD-Überlauf-Ziel eintrifft und nicht während des gesamten Rufzyklus. Wenn ein Anruf das UCD-Überlauf-Ziel verlässt, erklingt die Standard-Wartemusik.

Für jede UCD-Gruppe kann die maximale Anzahl der Anrufe in der Warteschlange individuell festgelegt 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.

14.6.8 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.

Sie haben die folgenden 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.

14.6.10 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.

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.

14.6.11 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).

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.

Zugehörige Konzepte

[Konfiguration der Teilnehmer](#) auf Seite 225

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.

Anmerkung: Standardmäßig gehört jeder Teilnehmer zur Berechtigungsgruppe 7; dies kann jedoch geändert werden. Darüber hinaus gehört auch jede Amtsleitung zur Berechtigungsgruppe 7, diese Einstellung ist aber nicht konfigurierbar. Daher sollten Sie die Berechtigungsgruppe 7 nicht verwenden und uneingeschränkten Zugriff (Vollamtszugriff) auf alle Bündel erlauben.

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.

15.1.2 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) 0800xx-Nummern zu berechtigen, muss hier lediglich die 0800 eingegeben werden. Da sich die Listen nur auf gehende Externengespräche 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

Leistungsmerkmal	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

15.1.3 Blacklist

Im OpenScape Business-System steht eine Blacklist zur Verfügung, die es ermöglicht, eingehende Anrufe von bestimmten Rufnummern (CLI) und von Anrufen ohne Rufnummer oder eingeschränkte Darstellung der Rufnummer zu blockieren.

Die Blacklist unterstützt bis zu 100 Nummern mit maximal 25 Ziffern, entweder im kanonischen Format (z.B. +4989) oder im internationalen Format (z.B. 004989). Unterstützte Zeichen sind die Ziffern 0-9 und das Zeichen "+". Das Zeichen "+" bezieht sich auf das internationale Präfix, das im System konfiguriert ist. Es muss immer an der ersten Stelle eingegeben werden. Nummernfragmente ab Beginn der Rufnummer (CLI) sind erlaubt. Bei der Eingabe einer Nummer in die Blacklist wird eine logische Prüfung durchgeführt. Die Nummer wird abgelehnt, wenn sie bereits eingegeben wurde oder wenn sie durch ein Zahlenfragment abgedeckt ist.

Die Überprüfung der übertragenen Anrufer-Nummern erfolgt immer im internationalen Format. Wenn Anrufer-Nummern in anderen Formaten übertragen werden, werden sie entsprechend den Routendaten in das internationale Format umgewandelt.

Die Blacklist wird auf alle im System konfigurierten Leitungen der Zentrale angewendet. Sie unterstützt mehrere Zentralstellen/Telefonie-Anbieter mit unterschiedlichen Landes- und Ortsvorwahlen.

Für jeden gesperrten Anruf wird von der Blacklist ein Ereignisprotokolleintrag erstellt.

Innerhalb eines OpenScape Business-Netz muss die Blacklist in jedem Knoten, der mit der Zentralstelle/den Telefonie-Anbietern verbunden ist, bzw. in den Gateways konfiguriert werden. Interne Anrufe im Netz werden durch die Blacklist nicht eingeschränkt.

Die Blacklist kann vom Systemadministrator aktiviert/deaktiviert werden. Zusätzlich kann ein separates Flag für die Sperrung von anonymen Anrufen gesetzt werden.

Serviceprotokolle enthalten Informationen über blockierte angerufene Nummern. Protokolleinträge, die blockierten angerufenen Nummern entsprechen, enthalten den EventText **!BlackListed Call**. Um die angerufene Nummer zu finden, die gesperrt wurde, überprüfen Sie die letzten beiden Ziffern des Protokolleintrags. Diese Ziffern (in hexadezimaler Form) entsprechen der Position in der Blacklist, in der die gesperrte Nummer enthalten ist. Wenn diese Ziffern ff sind, dann ist der blockierte Anruf anonym.

Abhängigkeiten

Anrufe mit CLI-Unterdrückung werden vom System nicht als anonyme Anrufe blockiert, wenn das Flag **Rufnummern-Unterdrückung ignorieren** innerhalb des Systems gesetzt ist. Die Rufnummer des Anrufers muss in diesem Fall explizit in die Blacklist eingetragen werden. Das Flag **Rufnummern-Unterdrückung ignorieren** ist in der werkseitigen Voreinstellung deaktiviert. Es kann nur über den Manager E aktiviert werden.

Die Mobilitätsfunktion des Systems kann von der Blacklist gestört werden, wenn Handynummern von Mobility Teilnehmern in die Blacklist eingetragen werden. In diesem Fall wird der Anruf zum DISA Zugang im Call Through-Modus durch die Blacklist blockiert.

15.1.4 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.

Zeitgesteuerte Nachtschaltung

Variable Nachtschaltung

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.

Das Kommunikationssystem aktiviert und deaktiviert die Nachtschaltung nach einem vom Administrator festgelegten Zeitplan.

Tipp: 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.

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 kann eine individuelle Nachtschaltung konfiguriert werden. 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.

15.1.5 Automatische Berechtigungsumschaltung nach Zeit

Bei der automatischen Berechtigungsumschaltung nach Zeit werden die Teilnehmer in sogenannte Teilnehmer-Profilen zusammengefasst, in denen definiert ist, welche Berechtigungsgruppe in welchem Zeitintervall der Woche gültig ist. Für jedes Teilnehmer-Profil kann ein Zeitplan konfiguriert werden.

Abhängigkeiten

Unterschiede zwischen der automatischen Berechtigungsumschaltung nach Zeit und der zeitgesteuerten Nachtschaltung:

- Die automatische Berechtigungsumschaltung nach Zeit gilt nur für den Tag-betrieb 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.

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 Nachtschaltung funktionieren nicht knotenübergreifend.

15.1.5.1 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.

Anruf-Routing

	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday	Special da
00:00 am	CG 1	CG 1	CG 1	CG 1	CG 1	CG 1	CG 1	CG 1
01:00 am								
02:00 am								
03:00 am								
04:00 am			CG 3					
05:00 am			CG 3					
06:00 am			CG 3					
07:00 am			CG 3					
08:00 am	CG 2							
09:00 am	CG 2							
10:00 am	CG 2							
11:00 am	CG 2							
12:00 pm	CG 2							
01:00 pm	CG 2							
02:00 pm	CG 1							
03:00 pm								
04:00 pm								
05:00 pm								
06:00 pm								

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.

15.1.6 VBZ (Verkehrsbeziehungen)

Über das Leistungsmerkmal VBZ (Verkehrsbeziehungen) wird festgelegt, welche Teilnehmer des Kommunikationssystems Verbindungen zu welchen anderen Teilnehmern des Kommunikationssystems 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

Tipp: Das Leistungsmerkmal VBZ sollte nicht in Verbindung mit UC-Funktionalität genutzt werden, da es Einschränkungen zur Folge hätte.

15.1.6.1 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.

15.1.6.2 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 der VBZ-Gruppe 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

15.1.7 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).

15.1.8 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 Telefonschlusses 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.

15.1.9 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.

15.1.10 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.

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 beschrieben.

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 teurere) 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.

Tipp: Auch bei Kommunikationssystemen mit analogen Amtsleitungen (HKZ) muss eine Standortnummer konfiguriert werden (Ländervorwahl / ggf. Ortsnetzkennzahl / ggf. Anlagenrufnummer).

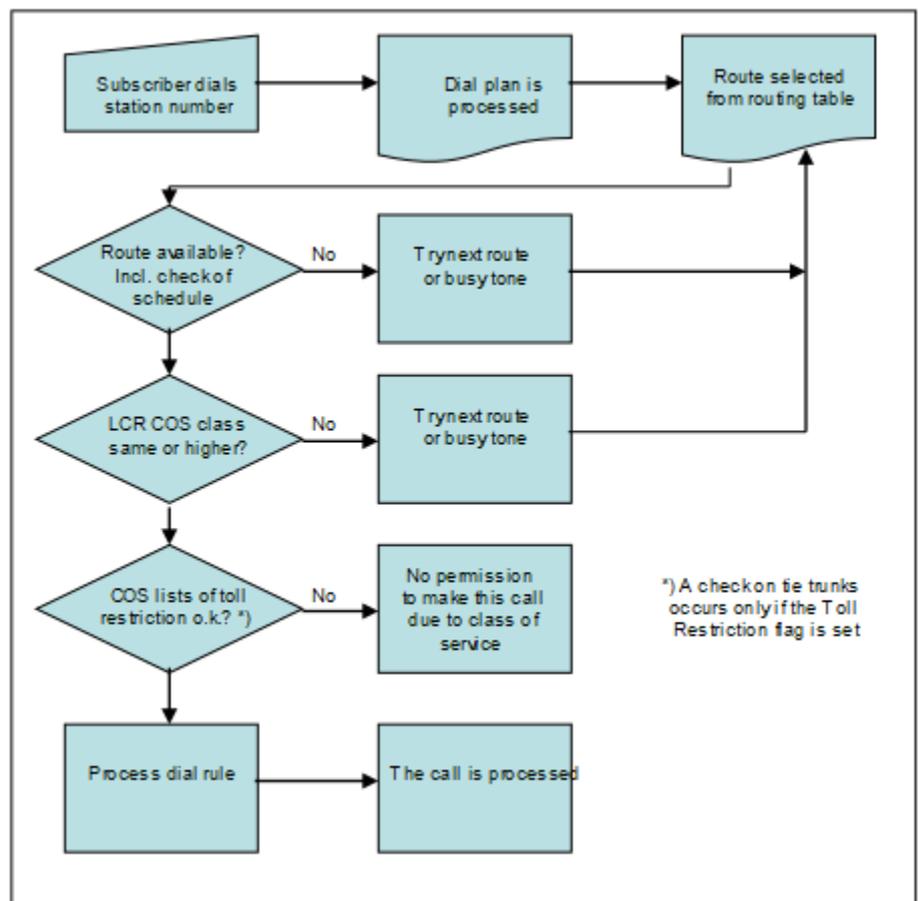
Darüber hinaus muss eine Durchwahlnummer oder, im Falle eine leeren Durchwahlnummerntabelle, eine Durchwahlnummer des eigenen analogen Amtsanschlusses (HKZ) konfiguriert werden. Nur so ist sichergestellt, dass alle externen Ziele erreicht werden können.

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 (KWZ)	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.

15.2.2 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 weiteren Parameter für diesen Verbindungsaufbau 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 und . . 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" gebildeten 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 Wählziffer 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 Default-Einträge im LCR-Wahlplan. Bis Wahlplan 34 werden systemseitige Einträge für Notrufe, Auskunft, Sonderrufnummern, Standard-Amtsbelegung für PSTN und ITSP, für UC Suite, Ansageanschluten 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. Daher ist sicherzustellen, dass die Standard-Amtsbelegung mit der Änderung der Standortnummer weiterhin funktioniert (wichtig bei Wahl mit öffentlichen Rufnummern).

Tipp: Ab LCR-Wahlplan 36 stehen Einträge zur freien Verfügung.

15.2.3 LCR-Wegetabelle

In den Wegetabellen der Leitweglenkung LCR wird nach einer passenden Richtung gesucht (jeder Leitung muss eine Richtung 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 (Class Of Service COS),
- die Möglichkeit zur Warnung vor einer teureren 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 (Class Of Service COS) 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.

15.2.4 LCR-Berechtigung

Jedem Teilnehmer wird eine eigene LCR-Berechtigung (Class Of Service COS) 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
Amtsberechtigung	Die Berechtigungen (Wahlkontrolle) ist vorrangig vor der LCR-Berechtigung. Die Berechtigung (Wahlkontrolle) kann für Querleitungen ein- und ausgeschaltet werden.
VBZ Gruppenuordnung	Eine Wahl erfolgt nur, wenn auch die VBZ-Matrix dies zulässt.

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):
P(n) darfin der Zeichenkette mehrmals vorkommen und an beliebigen Stellen stehen. P(n) darf von beliebigen anderen Parametern eingeschlossen sein. (1- bis 60-fache der systemweiten Pauseneinheit).
- 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).

15.2.6 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 öffentlichen 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) ausgewählt 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).

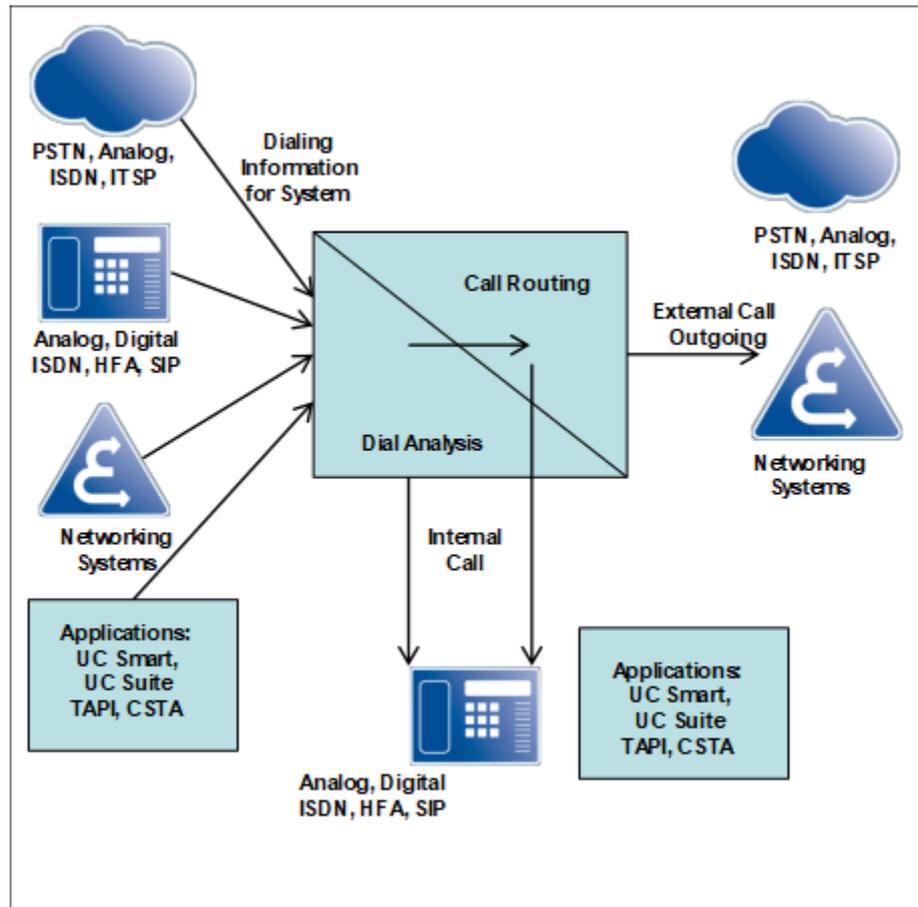
Standardmäßig wird eine Kennzahl (88) für eine gezielte Amtsbelegung über ISDN eingerichtet. Alle Kennzahlen können vom Administrator nachträglich eingerichtet bzw. geändert werden.

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: "+ 49nnn" wird zu "00049nnn", wobei die erste "0" den Hauptzugangscode der Telefonanlage repräsentiert)
- 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?)

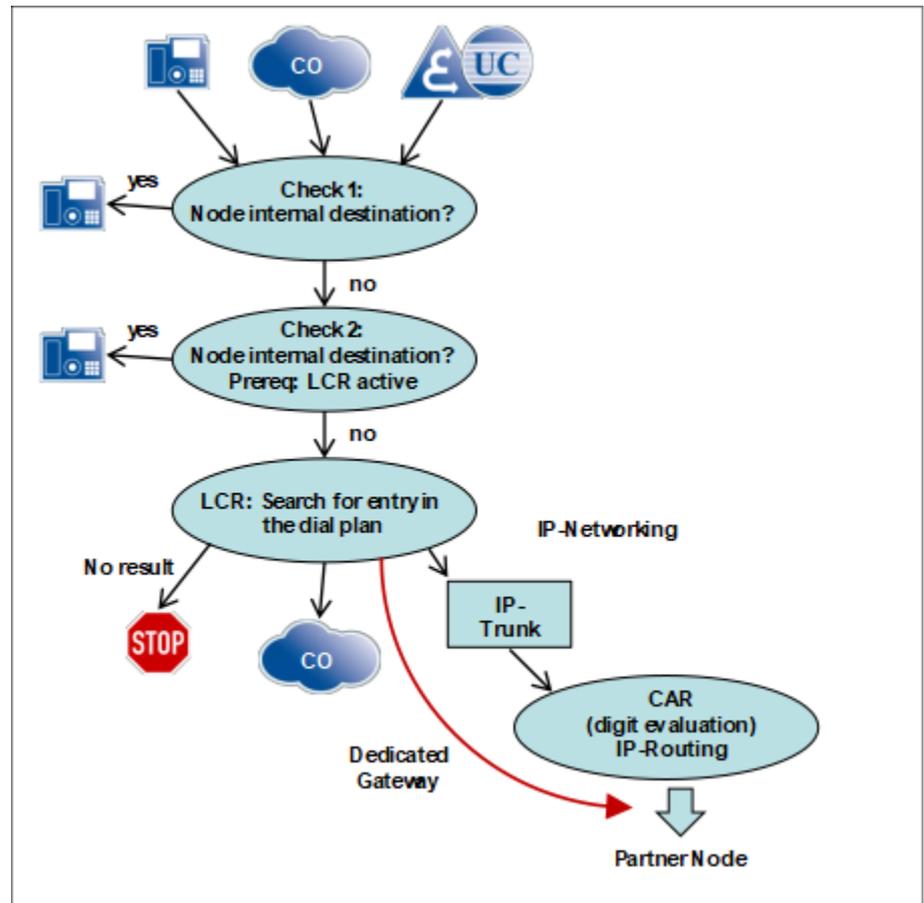
- Ziele mit kanonischer Rufnummer werden zunächst in wählbare Rufnummern (an der Teilnehmer-Schnittstelle) gewandelt, bzw. mit TON=International versehen (ITSP-Schnittstelle).
- Zielrufnummern von Leitung werden ggf. um den Rufnummernanteil der Anlagenrufnummer der entsprechenden Richtung gekürzt.
- Internrufe werden über den internen Wahlplan bewertet, Rufe von Extern durch den Wahlplan der Durchwahlrufnummern.

Prüfung 2 (Internes Rufziel?)

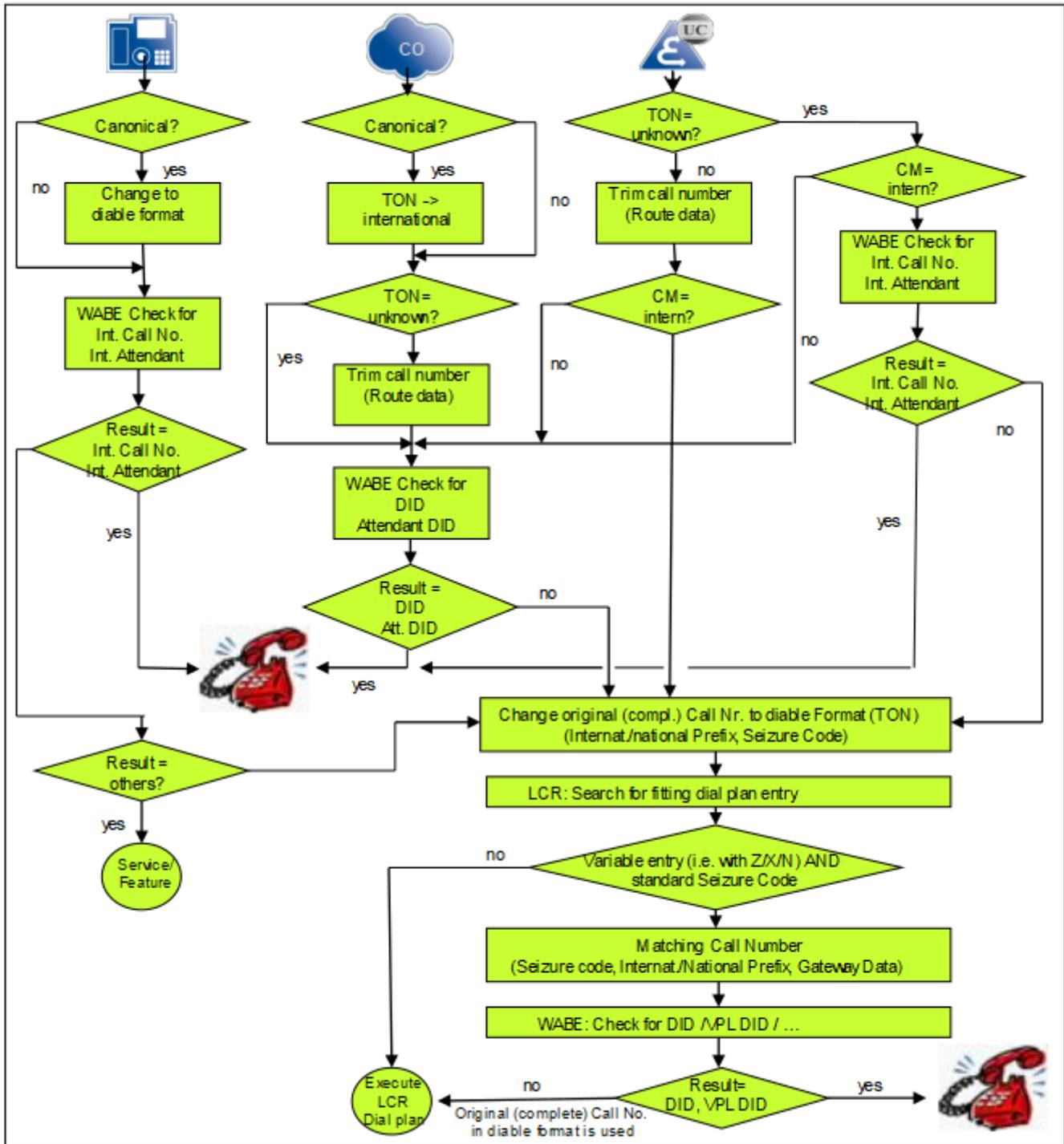
- Teilnehmer, Applikationen, Clients oder andere Kommunikationssysteme wählen Zielrufnummern im öffentlichen Format (z.B. 0 0049nnn)
- Bedingung: Standard-Amtskennzahl (z.B. "0") ist eingerichtet
- Zielrufnummer wird entsprechend der Anteile der Standortrufnummer (Gateway Standort) gekürzt und anhand des Wahlplans der Durchwahlrufnummern 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	Erklärung
WABE		Wahlbewertung
CM	CM	Classmark, kennzeichnet den Rufer als externen Rufer oder (netz-)internen Rufer

Deutsch	Englisch	Erklärung
TON	TON	Type Of Number Rufnummerentyp: Unknown, Subscriber (Teilnehmer), National oder International und wird sowohl bei Zielrufnummern als auch bei Ursprungsrufnummern verwendet.
DuWa	DuWa	Durchwahlrufnummer
TNR RNR	Int. Rufnr.	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.

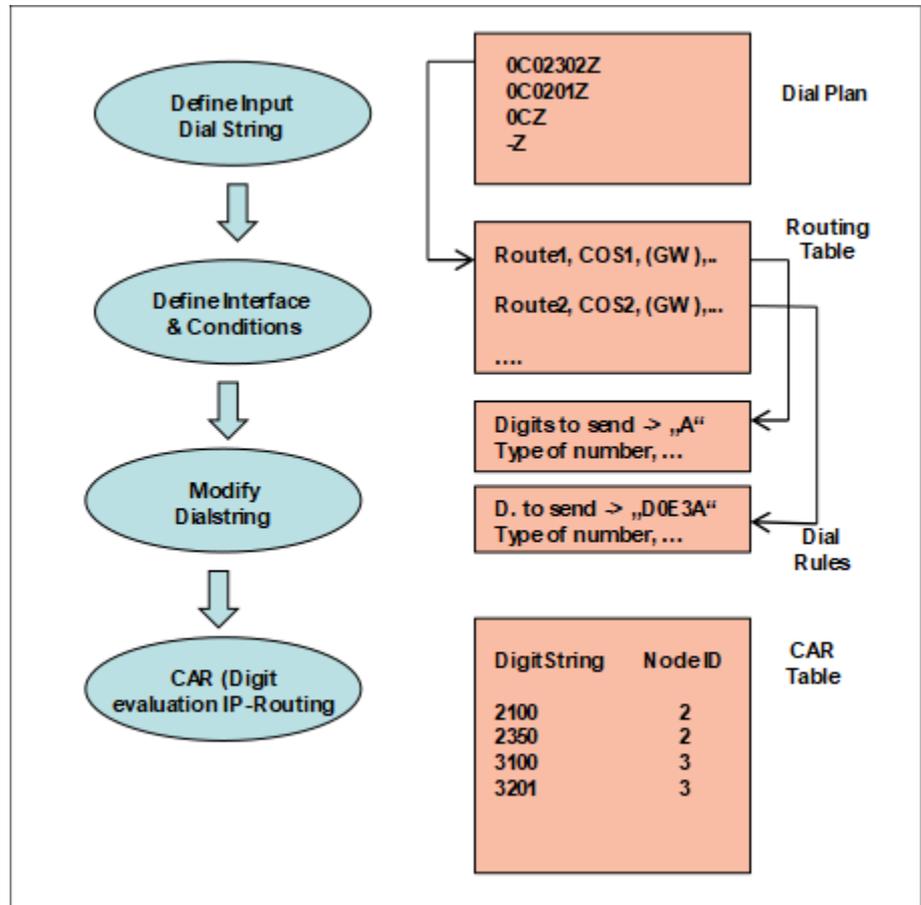
Die UC-Suite verhält sich bzgl. der Wahlbewertung wie ein SIP-Q-Trunk.

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

LCR-Einträge bei der Ersteinrichtung



Die Einträge in der Wegetabelle (Routing table) werden, wenn keine erfolgreiche Leitungsbelegung erfolgt, nacheinander in einer Schleife abgearbeitet.

Anmerkung: Bei Standalone-Systemkonfigurationen muss die Regel -z entfernt werden.

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 internationalen 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).

Tipp: 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?

Wie können Ziele per Konfiguration, dauerhaft eingerichtet werden?

Anwendungsfälle für ein dediziertes Gateway

Das dedizierte Gateway im WBM

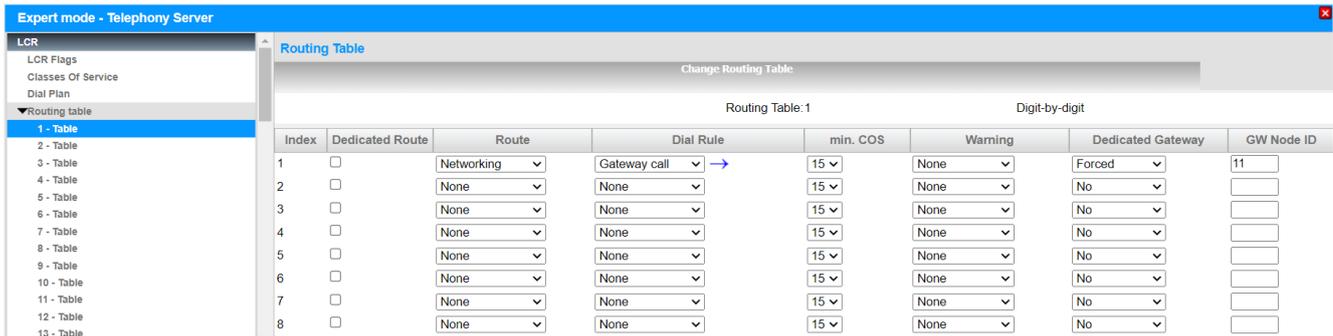
Folgende Werte können eingestellt werden:

- 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 knoten-individuelles Routing möglich (z.B. "0" zum jeweils zugehörigen Gateway-Knoten)
- 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).

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 Ursprung in einer Multi Gateway Konfiguration NICHT einem bestimmten Gateway zugeordnet werden können (z.B. die Faxgruppe eines UC Contact Centers)

Anruf-Routing



Nein	Die Rufnummernbewertung erfolgt anhand der CAR-Tabellen (keine GW Knoten-ID erforderlich)
Erzungen	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

Vernetztes System als Unteranlage (ohne Amtsleitung)

Netzverbund mit Multi Gateway

- 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:

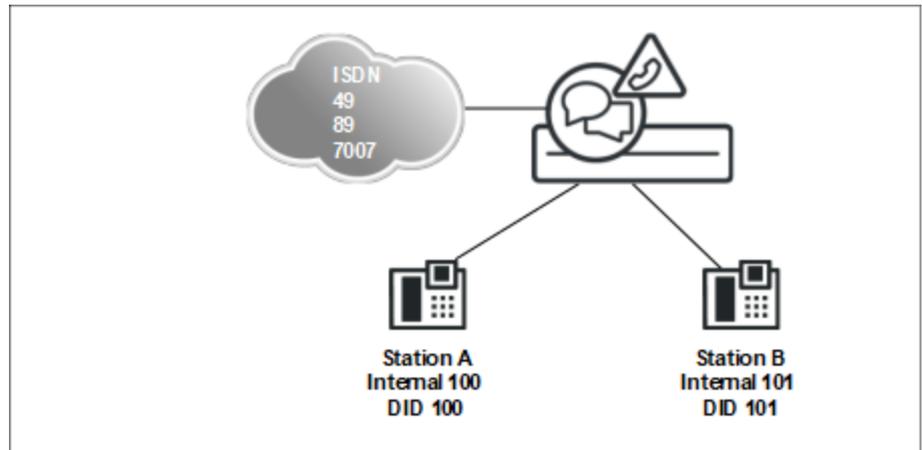
2 Amtsrichtungen

- 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

- 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

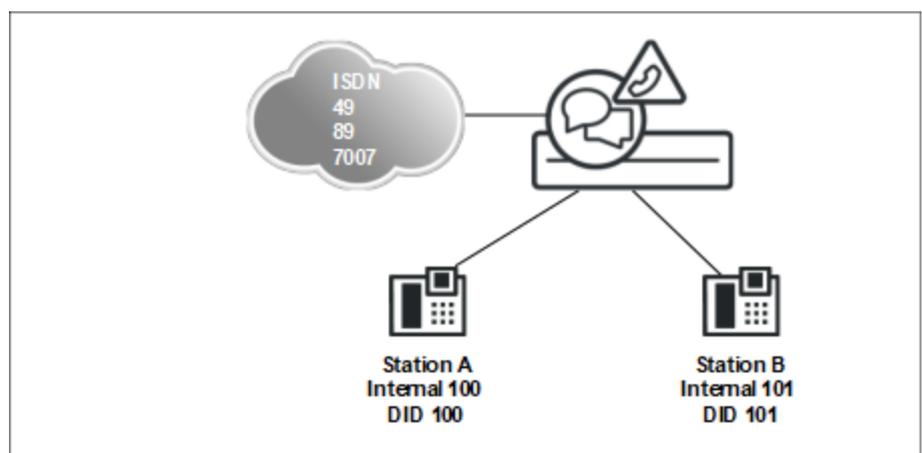


Box	Slot	Callno	Name	DID	Type
1	1	100	-	100	System Client
1	1	101	-	101	System Client

15.3.4.2 Teilnehmer A ruft Teilnehmer B über öffentliche Rufnummer

Konfiguration

Abhängigkeiten der "Standortnummer" (Gateway Location)



Der Anruf wird system-intern zugestellt, da die Zielrufnummer ein DID-Teilnehmer des eigenen Systems ist.

Anruf-Routing

	Box	Slot	Callno	Name	DID	Type
	1	1	100	-	100	System Client
	1	1	101	-	101	System Client

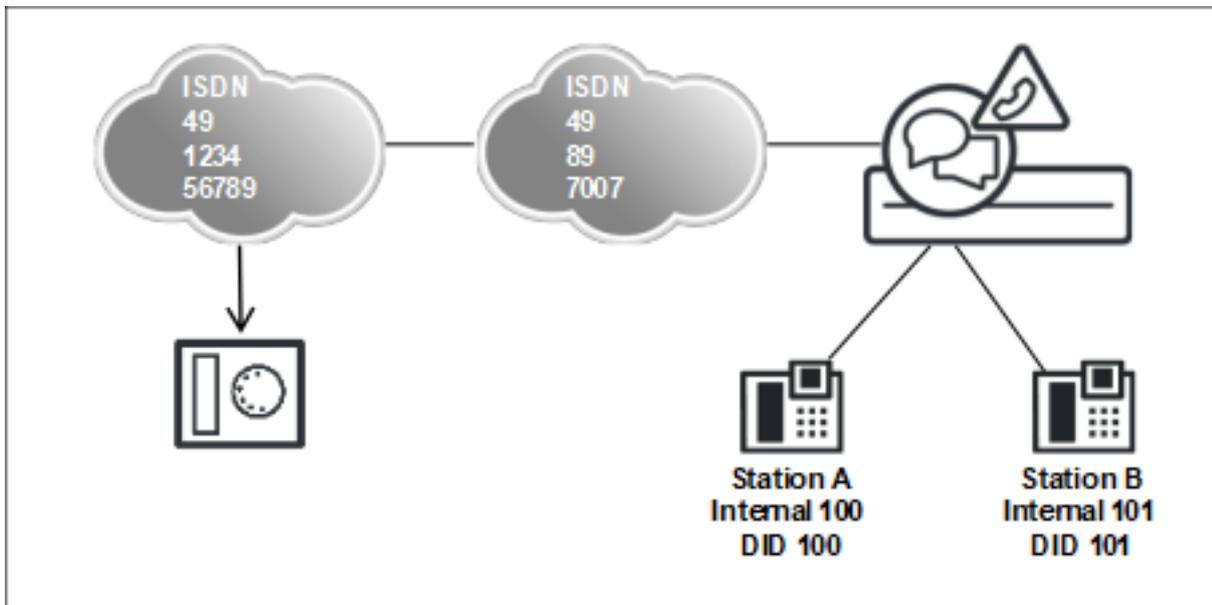
Nachdem die Zielrufnummer anhand der Gateway Location abgestrippt wurde, wird mit der abgestrippten Rufnummer im DID-(DUWA-)Rufnummernplan nach einem Ziel gesucht.

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 vorgelegten 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 eigenen Kommunikationssystem liegt.

Zusätzlich zu den Daten des vorherigen Szenarios "Teilnehmer A ruft Teilnehmer B über öffentliche Rufnummer" muss im LCR ein geeigneter Wahlplan-Eintrag zur Belegung der Amtsleitung vorhanden sein (z.B. "OCZ").

Die LCR-Wegetabelle und der Wahlplan müssen dem entsprechend eingerichtet sein.

Expert mode - Telephony Server

LCR

LCR Flags

Classes Of Service

Dial Plan

Change Dial Plan

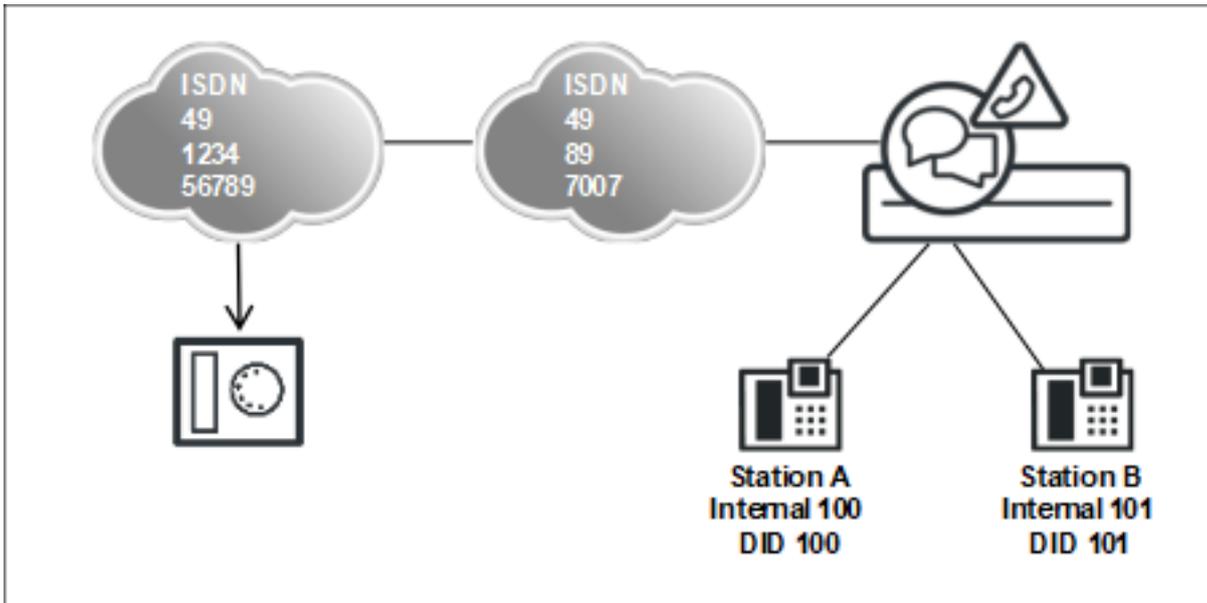
Display Dial Plan

Dial Plan	Name	Dialed digits	Routing Table	Acc. code	Classes of service	Emergency
1	Notruf	0C112	4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	Notruf	0C110	4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	Televoting	0C0137Z	4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	Televoting	0C0138Z	4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5	Premium Dienste	0C0900Z	4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6	Auskunftsdienst	0C118Z	4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7	Sonderrufnummer	0C116Z	4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8	Sonderrufnummer	0C115	4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
9	Preselection	0C010Z	4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
10	Sonderrufnummer		4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
11	Sonderrufnummer		4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
12	Sonderrufnummer		4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
13	Sonderrufnummer		4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
14	Sonderrufnummer		4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
15	Sonderrufnummer		4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
16	Services	0CZ	4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
17	National	0C0-Z	4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
18	Local	0C1Z	5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
19	Local	0CNZ	5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
20	International	0C00-Z	4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
21	Sipgate	855CZ	4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
22	Sipgate	855C0-Z	4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
23	Sipgate	855C1Z	5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
24	Sipgate	855CNZ	5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
25	Sipgate	855C00-Z	4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
26	Standard	856CZ	6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
27	Standard	856C0-Z	6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
28	Standard	856C1Z	6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
29	Standard	856CNZ	6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Page 1 of 10

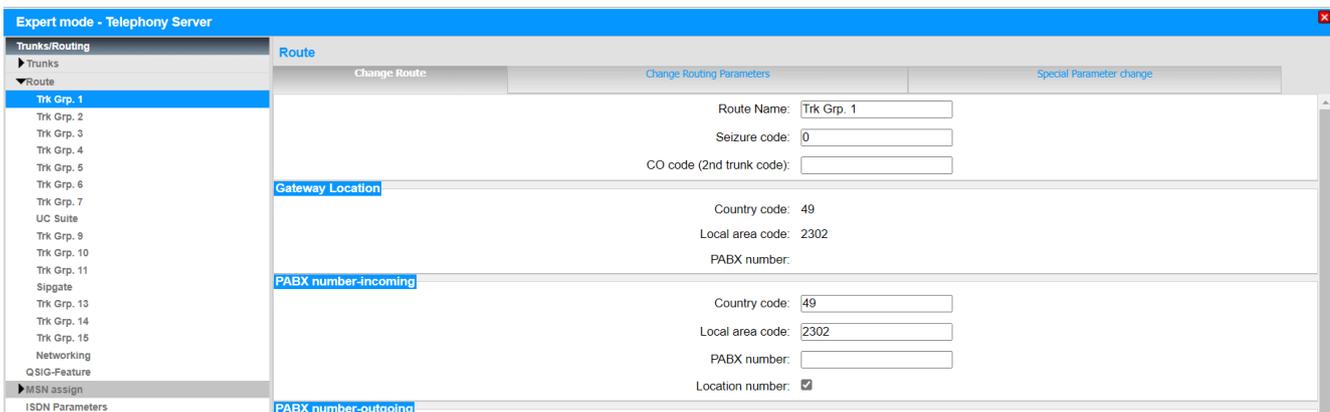
Apply Undo Help

15.3.4.4 ISDN-Amt ruft Teilnehmer A



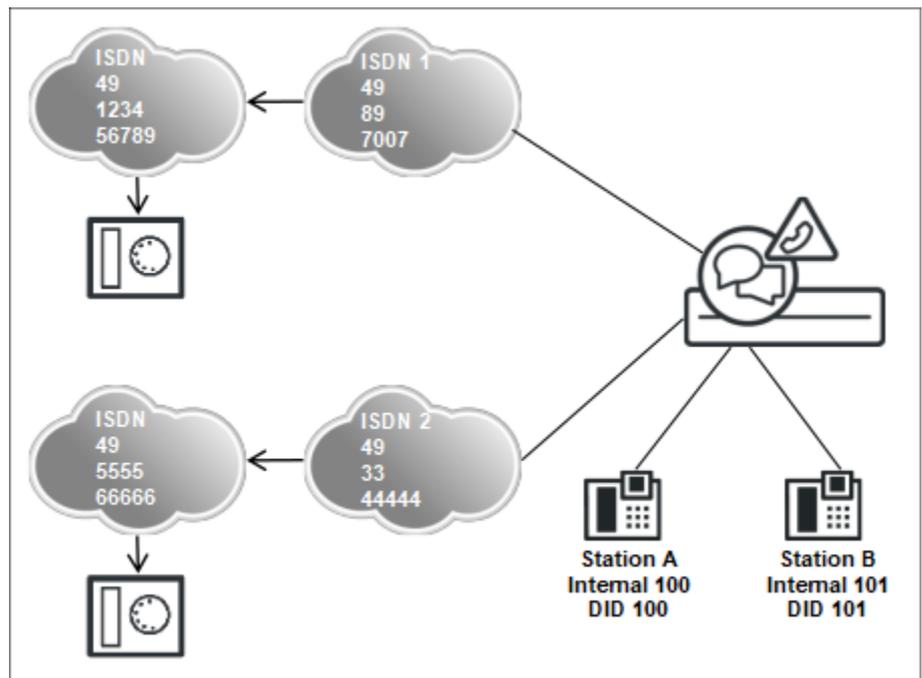
Bei einem kommenden Anruf über ISDN-Trunk wird die Zielrufnummer anhand der Konfigurationsdaten der Anlagenrufnummer kommend (PABX number incoming) der Richtung abgestrippt. Mit dem verbleibenden Rest der Zielrufnummer (Duwa) wird nach einem Ziel im Duwa-Wahlplan gesucht.

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 TIn über Amtsanschluß 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.

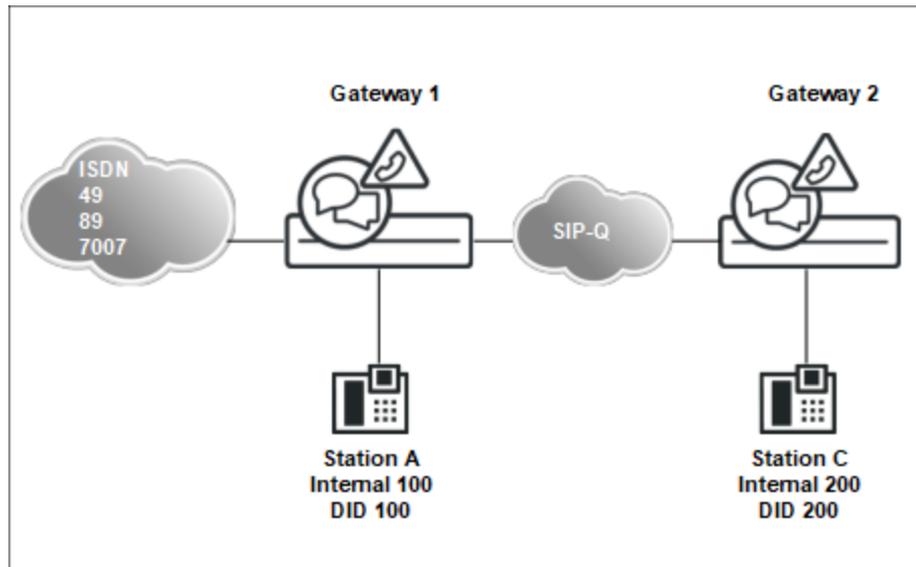
Hinweise bzw. Einschränkungen:

- 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)

Anruf-Routing



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 Grundinstallation der Systeme 1 und 2: Bei der Nummerierung der Standalone-Systeme muss die geschlossene Nummerierung im zukünftigen Netzverbund berücksichtigt werden.
- 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.

The screenshot shows the configuration wizard for a network integration. The steps are: 1. System Overview, 2. Central Functions for Stations, 3. ISDN Configuration, 4. Configure Internet Access, 5. Provider configuration and activation for Internet Telephony, 6. Select a station, 7. Configured Stations, 8. SmartVM, 9. Configure MeetMe Conference, 10. Configure E-Mail Forwarding. The current step is 'Network Parameters'. The 'Network Integration' checkbox is checked. The 'Node ID' is set to 1. The 'PABX number' section shows 'Country code: 00 49 (mandatory)', 'Local area code: 0 89 (optional)', and 'PABX number: 7007 (optional)'. The 'International Prefix' is set to 00.

Starten Sie den Netzwerk-Wizard in System 1. Dieses System (dieser Knoten) wird als 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 Netzwerk befindet, sollte diese bevorzugt zum Master erklärt werden (Bandbreite, Performance).

Node type

If a network is configured, one system, and only one, in the network must be a MASTER node.

This system is the MASTER node

This system is a SLAVE node

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.

Node Input

Enter the IP addresses of the corresponding OpenScape Business systems in the domain.
The Application Server IP address can be the IP address of an application board or a connected OSBiz UC BS.

NodeId	OSBiz X / OSBiz S	Net Name	Type	Application Server	Encryption	Registration Status
1	192.168.186.13	Master	V2 Mainboard	<input type="checkbox"/>	<input type="checkbox"/>	✓
2	192.168.186.14	Slave	V3 Mainboard Basic	<input type="checkbox"/>	<input type="checkbox"/>	-

Delete

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 **Experten-Modus > Sprachgateway > Networking > Routing** möglich.

Die Übersicht über die automatische Synchronisierung im Netzwerk 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 Netzwerk

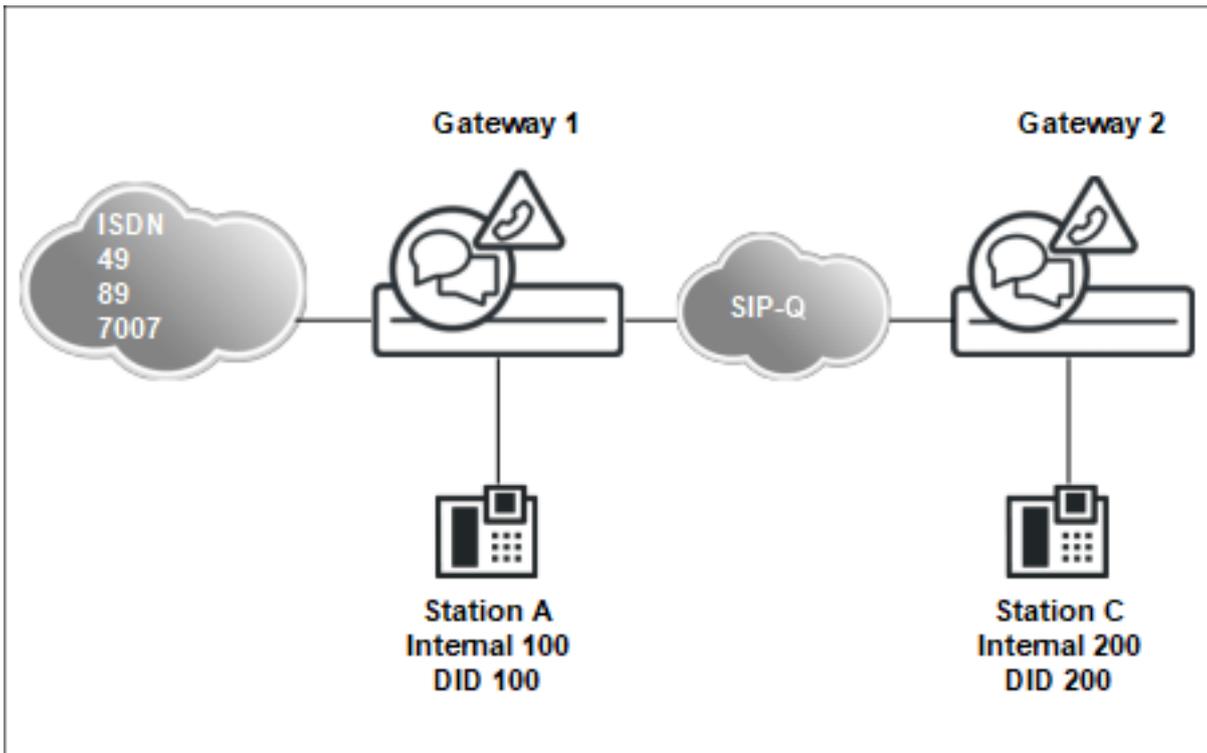
Vernetztes Kommunikationssystem als Unteranlage

**Konfiguration von Knoten 1, Einrichtung im LCR über
Dediziertes Gateway**

**Konfiguration von Knoten 2, Einrichtung der Richtung
"Networking"**

**Konfiguration von Knoten 2, Einrichtung der Standortnummer
an der "Dummy-Amtsrichtung"**

**Konfiguration von Knoten 2, Einrichtung im LCR über
dediziertes Gateway**



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.

Anmerkung: 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.

Expert mode - Telephony Server

LCR

- LCR Flags
- Classes Of Service
- Dial Plan**
- Routing table
 - 1 - Table
 - 2 - Table
 - 3 - Table
 - 4 - Table
 - 5 - Table
 - 6 - Table

Dial Plan

Change Dial Plan

Dial Plan	Name	Dialed digits	Routing Table	Acc. code	Classes of service	Emerg
76	System 2 DialInt	0C0049897007-2XX	40 →	<input type="checkbox"/>	<input checked="" type="checkbox"/>	[...]
77	System 2 DialNat	0C0897007-2XX	40 →	<input type="checkbox"/>	<input checked="" type="checkbox"/>	[...]
78	System 2 DialSub	0C7007-2XX	40 →	<input type="checkbox"/>	<input checked="" type="checkbox"/>	[...]
79			- →	<input type="checkbox"/>	<input checked="" type="checkbox"/>	[...]
80			- →	<input type="checkbox"/>	<input checked="" type="checkbox"/>	[...]

Expert mode - Telephony Server

Routing Table

Change Routing Table

Routing Table: 40

Digit-by-digit

Index	Dedicated Route	Route	Dial Rule	min. COS	Warning	Dedicated Gateway	GW Node ID
1	<input type="checkbox"/>	Networking	Dial Rule 40 →	15	None	Forced	2

Expert mode - Telephony Server

LCR

- LCR Flags
- Classes Of Service
- Dial Plan
- Routing table
- Dial rule**
- Multistate

Dial Rule

Change Dial Rule

	Rule Name	Dial rule format	Network access	Type
5	IP-Network	A	Corporate Network	Unknown
6	Multi-Location	BA	Corporate Network	Unknown
7	Gateway call	E1A	Corporate Network	Unknown
8	COInternat	D0E4A	Main network supplie	Unknown
9	Add_cc_to_Canoni	D49E2A	Main network supplie	Country code
10	National_to_Cano	D49E3A	Main network supplie	Country code
11	Internat_to_Can	E3A	Main network supplie	Country code
12	SIP local_Canoni	HE2A	Main network supplie	Country code
13	networking_ext	D855019036691007	Main network supplie	Unknown
14			Unknown	Unknown
15			Unknown	Unknown
16			Unknown	Unknown
17			Unknown	Unknown
18			Unknown	Unknown
19			Unknown	Unknown
20			Unknown	Unknown
21			Unknown	Unknown
22			Unknown	Unknown
23			Unknown	Unknown
24			Unknown	Unknown
25	Dialrule 40	D49897007E3A	Corporate Network	Country code

Expert mode - Telephony Server

Trunks/Routing

- Trunks
- Route**

Route

Change Route

Change Routing Parameters

Special Parameter change

Route Name: Networking

Seizure code:

CO code (2nd trunk code):

Gateway Location

Country code: 49

Local area code: 89

PABX number: 7007

PABX number-incoming

Country code:

Local area code:

PABX number:

Location number:

Anruf-Routing

In der Registerkarte **Richtungsparameter ändern** ist die Richtungsart **PABX** einzutragen.

Expert mode - Telephony Server

Trunks/Routing

Route

Change Route: Change Routing Parameters: Special Parameter change

Route Name: Dummytrunk

Seizure code: 0

CO code (2nd trunk code):

Gateway Location

Country code: 49

Local area code: 89

PABX number: 7007

PABX number-incoming

Country code: 49

Local area code: 89

PABX number: 7007

Location number:

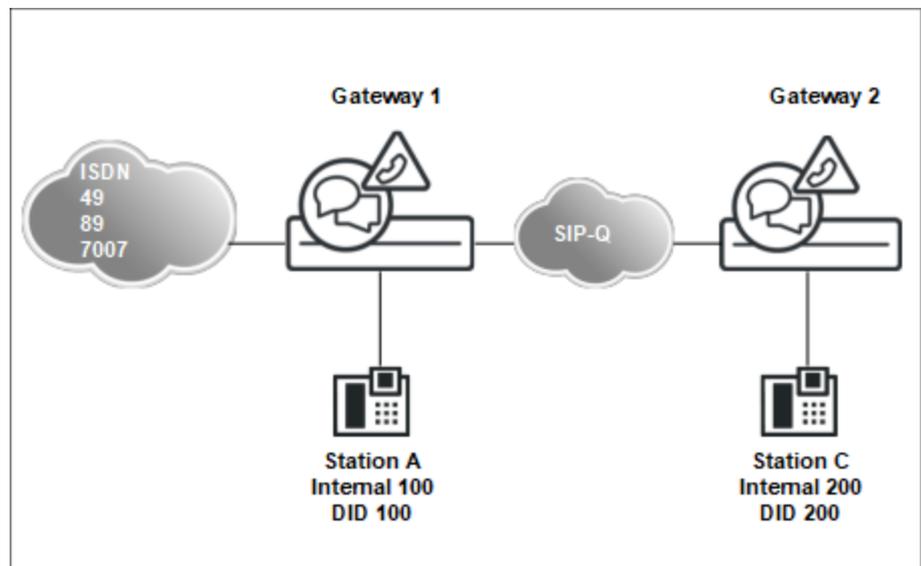
In der Registerkarte **Richtungsparameter ändern** ist die Richtungsart **Amt** einzutragen.

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

Besonderheiten dieser Konfiguration



Beispiel: Kommender Anruf mit Zielrufnummer mit TON = Teilnehmer

- 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.

Tipp: 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.

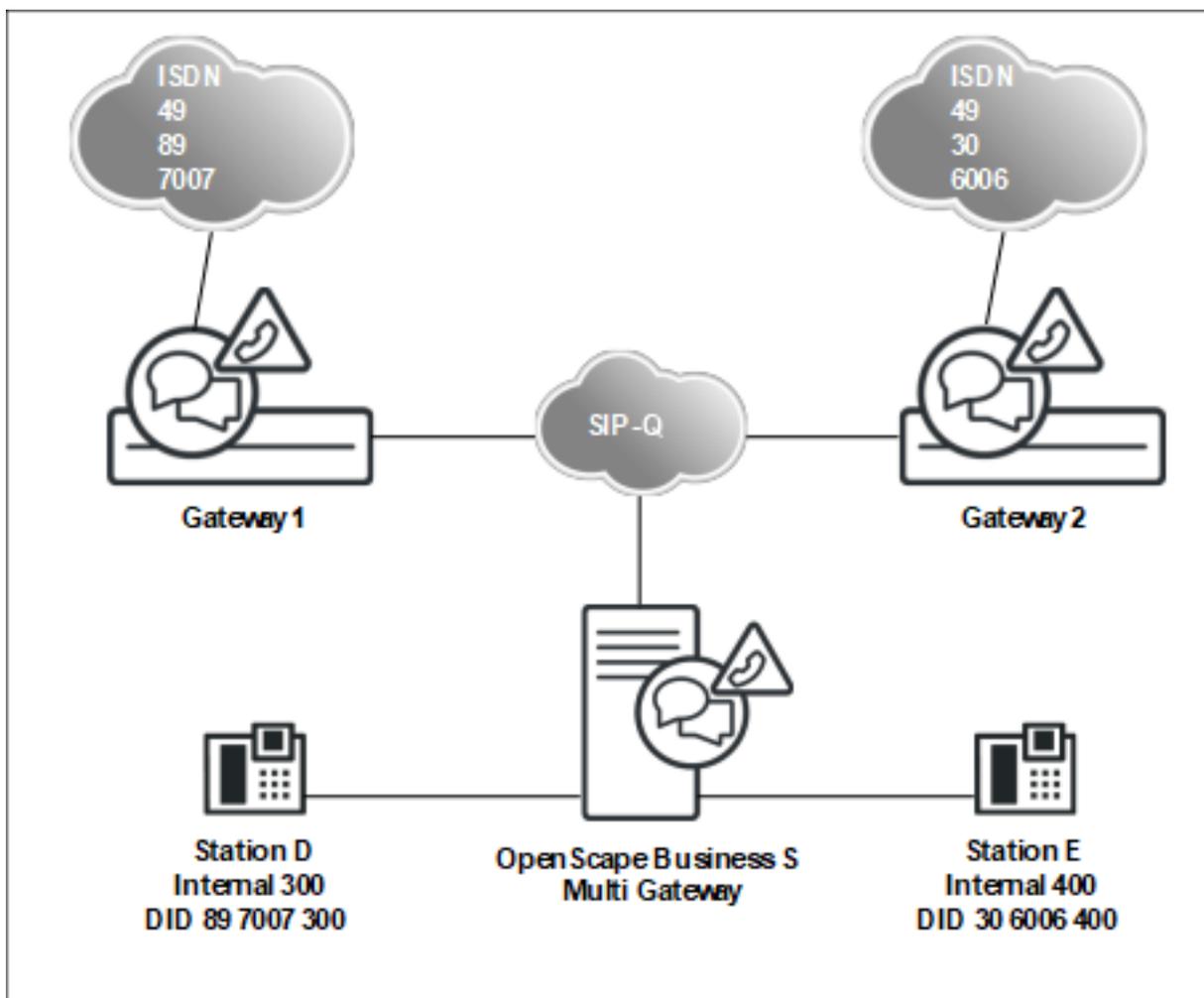
- Knoten 2 ist ebenfalls, wie im vorherigen Szenario beschrieben, einzurichten.

15.3.4.9 ISDN-Amt Gateway 1 ruft Teilnehmer D

Vernetztes System in einer Multi Gateway Konfiguration

Konfiguration

Konfiguration des Multi Gateway, OpenScape Business S



Beispiel: Kommender Anruf mit Zielrufnummer mit TON = Teilnehmer Besonderheiten in diesem Szenario:

Anruf-Routing

- 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

PABX number

Country code: 00 (mandatory)
 Local area code: 0 (optional)
 PABX number: (optional)

General

International Prefix:

Network Parameters

Network Integration:
 Node ID:

Netzwerk-Wizard für Gateway 1

Node type

If a network is configured, one system, and only one, in the network must be a MASTER node.

This system is the MASTER node
 This system is a SLAVE node

Enter the IP address of the MASTER node:

After 'OK & Next' you cannot undo the action by aborting the wizard.

Expert mode - Telephony Server

LCR
 LCR Flags
 Classes Of Service
 Dial Plan
 Routing table
Dial rule
 Multisite

Dial Rule

Change Dial Rule

	Rule Name	Dial rule format	Network access	Type
1	ISDN	A	Main network supplie	Unknown
2	SIP	A	Main network supplie	Unknown
3	SIP lokal	HE2A	Main network supplie	Unknown
4	MEB	E1A	Corporate Network	PABX number
5	IP-Network	A	Corporate Network	Unknown
6	Multi-Location	BA	Corporate Network	Unknown
7	Gateway call	E1A	Corporate Network	Unknown
8	COInternat	D0E4A	Main network supplie	Unknown
9	Add_cc_to_Canoni	D49E2A	Main network supplie	Country code
10	National_to_Cano	D49E3A	Main network supplie	Country code
11	Internat_to_Can	E3A	Main network supplie	Country code
12	SIP lokal_Canoni	HE2A	Main network supplie	Country code
13	networking_ext	D855019036691007	Main network supplie	Unknown
14	Node 2 open Num	E1A	Unknown	Unknown
15			Unknown	Unknown

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.

- 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

Setup - Wizards - Basic Installation - Basic Installation

1 System Overview 2 Central Functions for Stations 3 Provider configuration and activation for Internet Telephony 4 Select a station 5 Configured Stations 6 Automatic Configuration of Application Suite 7 Configure MeetMe Conference 8 Configure E-Mail Forwarding

Note: changes done in expert mode must be reviewed/repeated after running through the wizard.
 Note: At least the configuration of the 'Country code' is needed for features such as 'Internet telephony' and 'MeetMe conference'.
 If you want your OpenScape Business in "OpenScape Business Network Integration" you should select the "Network Integration" check box and enter a node ID. In this case, make sure that this node ID is unique within the whole network integration.
 Normally, this integration is done by a Service Technician.
 For a standalone OpenScape Business clear the 'Network Integration' check box.

PABX number

Country code: 00 (mandatory)
 Local area code: 0 (optional)
 PABX number: (optional)

General

International Prefix:

Network Parameters

Network Integration:
 Node ID:

Tip: 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

Node input

Enter the IP addresses of the corresponding OpenScape Business systems in the domain.
 The Application Server IP address can be the IP address of an application board or a connected OSBiz UC BS.

	Nodeid	OSBiz X / OSBiz S	Net Name	Type	Application Server	Encryption	Registration Status
<input type="button" value="Delete"/>	<input type="text" value="1"/>	<input type="text" value="172.30.111.22"/>	<input type="text" value="Slave"/>	<input type="text" value="V3 Mainboard Basic"/>		<input type="checkbox"/>	<input type="checkbox"/>
	<input type="text" value="2"/>	<input type="text" value="192.168.186.13"/>	<input type="text" value="Master"/>	<input type="text" value="V2 Mainboard"/>		<input type="checkbox"/>	<input checked="" type="checkbox"/>

Wählen Sie Multi Gateway in der Netzwerk-Konfiguration aus.
 Richtungen der OpenScape Business S, Multi Gateway

Trunks/Routing

- Trunks
- Route
 - route 1
 - Trk Grp. 2
 - Trk Grp. 3
 - Trk Grp. 4
 - Trk Grp. 5
 - Trk Grp. 6
 - Trk Grp. 7
 - App. Suite
 - Trk Grp. 9
 - Trk Grp. 10
 - Trk Grp. 11
 - Sippgate
 - Trk Grp. 13
 - Trk Grp. 14
 - Trk Grp. 15
 - Networking

Route

Change Route Change Routing Parameters Special Parameter change

Route Name:
 Seizure code:
 CO code (2nd trunk code):

Gateway Location

Country code: 49
 Local area code:
 PABX number:

PABX number-incoming

Country code:
 Local area code:
 PABX number:

PABX number-outgoing

Location number:

Der Country Code wurde bereits im wizard eingetragen.
 Richtungsparameter: Richtungsart Amt
 Diese Richtung bekommt die Richtungsart "Amt".

Anruf-Routing

The screenshot displays the configuration for a route named 'Networking'. The interface is organized into several sections:

- Change Route:** Route Name: Networking
- Change Routing Parameters:** Seizure code: [] CO code (2nd trunk code): 0
- Gateway Location:** Country code: 49 Local area code: [] PABX number: []
- PABX number-incoming:** Country code: [] Local area code: [] PABX number: [] Location number:
- PABX number-outgoing:** Country code: [] Local area code: [] PABX number: [] Suppress station number:
- Overflow route:** Overflow route: None

Routing Parameter: Rufnummerntyp outgoing=National, Richtungsart PABX

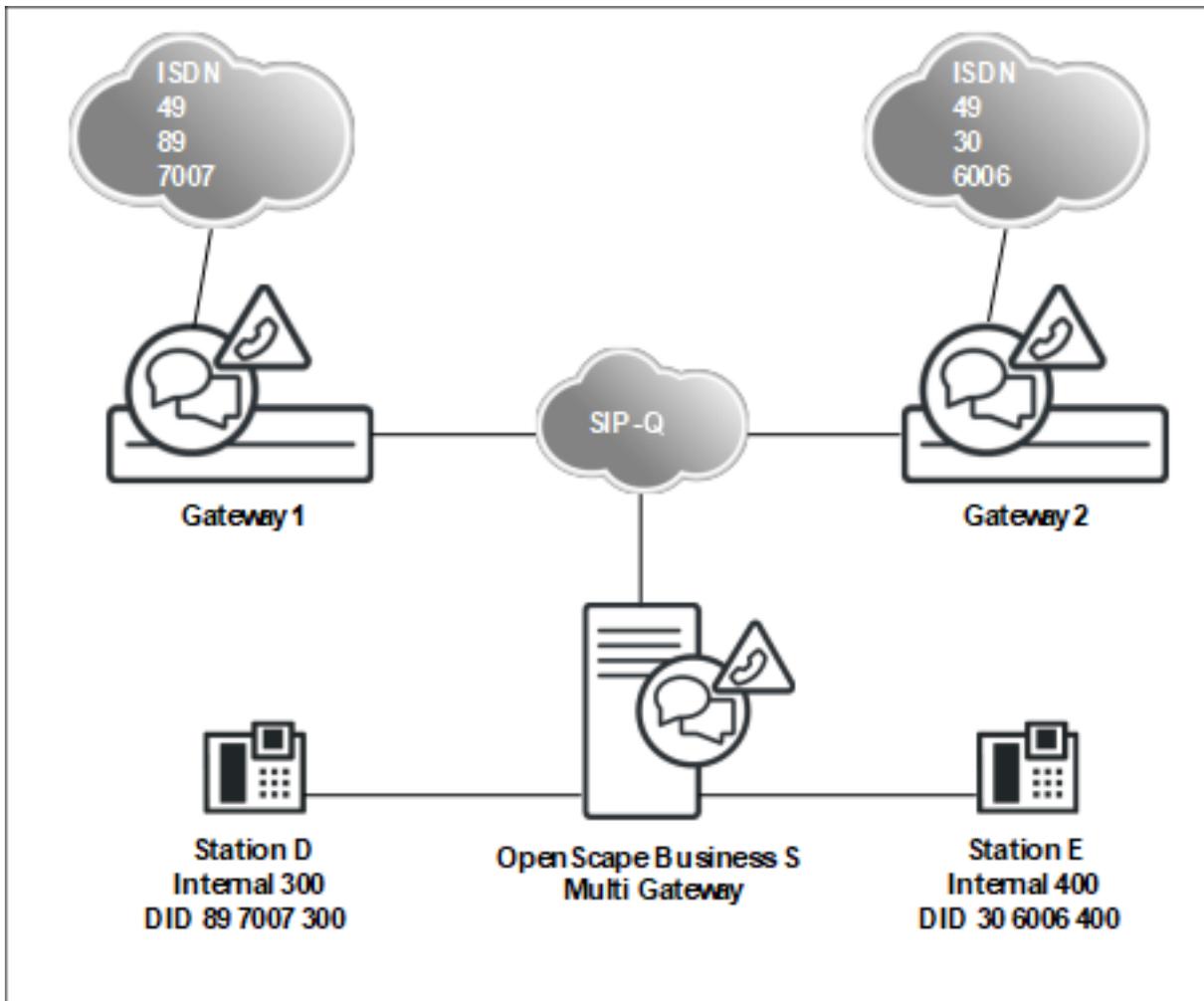
Diese Richtung bekommt die Richtungsart „PABX“ und der NR-Typ gehend ist mit **Ortsnetzkenzahl** einzurichten.

15.3.4.10 Teilnehmer D ruft externen Teilnehmer über Amt

Vernetztes System in Multi Gateway Konfiguration

Konfiguration der OpenScape Business S, Multi Gateway

Routing der OpenScape Business S, Multi Gateway, zu den Gateways



Expert mode - Telephony Server

LCR
 LCR Flags
 Classes Of Service
 Dial Plan
 Routing table
Dial rule
 Multisite

Dial Rule
 Change Dial Rule

	Rule Name	Dial rule format	Network access	Type
1	ISDN	A	Main network supplie	Unknown
2	SIP	A	Main network supplie	Unknown
3	SIP lokal	HE2A	Main network supplie	Unknown
4	MEB	E1A	Corporate Network	PABX number
5	IP-Network	A	Corporate Network	Unknown
6	Multi-Location	BA	Corporate Network	Unknown
7	Gateway call	E1A	Corporate Network	Unknown

Anruf-Routing Notrufe

Index	Dedicated Route	Route	Dial Rule	min. COS	Warning	Dedicated Gateway	GW Node ID
1	<input type="checkbox"/>	Networking	Gateway call →	15	None	Multi-location	<input type="text"/>
2	<input type="checkbox"/>	None	None	15	None	No	<input type="text"/>
3	<input type="checkbox"/>	None	None	15	None	No	<input type="text"/>
4	<input type="checkbox"/>	None	None	15	None	No	<input type="text"/>
5	<input type="checkbox"/>	None	None	15	None	No	<input type="text"/>
6	<input type="checkbox"/>	None	None	15	None	No	<input type="text"/>
7	<input type="checkbox"/>	None	None	15	None	No	<input type="text"/>
8	<input type="checkbox"/>	None	None	15	None	No	<input type="text"/>
9	<input type="checkbox"/>	None	None	15	None	No	<input type="text"/>
10	<input type="checkbox"/>	None	None	15	None	No	<input type="text"/>
11	<input type="checkbox"/>	None	None	15	None	No	<input type="text"/>
12	<input type="checkbox"/>	None	None	15	None	No	<input type="text"/>
13	<input type="checkbox"/>	None	None	15	None	No	<input type="text"/>
14	<input type="checkbox"/>	None	None	15	None	No	<input type="text"/>
15	<input type="checkbox"/>	None	None	15	None	No	<input type="text"/>
16	<input type="checkbox"/>	None	None	15	None	No	<input type="text"/>

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.

Voraussetzungen

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

Fall 1: Wahl des Notrufs über PSTN-Leitung

Fall 2: Wahl des Notrufs über ITSP

Fall 3: Spezielle Vereinbarung mit ITSP oder PSTN-Providern

Fall 4: Notrufe bei Mobile Logon (IP-Mobility)

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.

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.

Nicht alle ITSPs unterstützen Notrufe. In diesem Fall muss per LCR-Konfiguration dafür gesorgt werden, dass Notrufe über PSTN geroutet werden.

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.

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.

Tipp: 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 nach Abnehmen des Hörers **keine** Möglichkeit, eine Rufnummer einzugeben. Vor Abnehmen des Hörers kann eine Rufnummer gewählt werden. 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 Rufweitschaltung 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

Themenbereich	Abhängigkeit
Anrufschutz	Ist beim Ziel der Anrufschutz aktiviert, hört der Anrufer den Besetztton.

15.4.2 Leitungstrennung für einen Notruf

Wird ein Notruf abgesetzt und keine Amtsleitung ist frei, dann wird eine Zwangstrennung ausgelöst. Dem notrufenden Teilnehmer wird automatisch die freie Leitung zugewiesen.

Die Leitungstrennung funktioniert bei ISDN- und ITSP-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.

15.4.3 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.

15.4.4 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

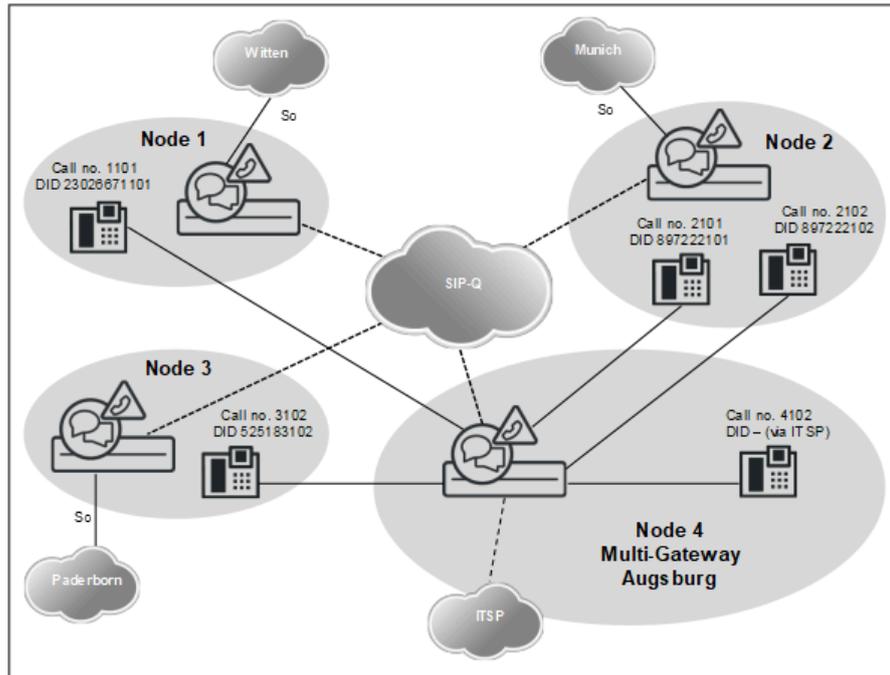
Wenn ein Teilnehmer eine Notrufnummer wählt (Kennung im LCR), überprüft ein Algorithmus, ob für das Telefon eine Notrufnummer konfiguriert wurde. Diese wird dann zur Erzeugung einer abgeleiteten Rufnummer verwendet, die im Netzverbund zum Routen des Anrufs über das richtige Gateway genutzt wird.

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.

Behandlung von Notrufnummern



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.
- 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, Ortsnetzkenzahl, Anlagenrufnummer) verglichen.

Falls unterschiedlich wird eine "lange" Notrufnummer gebildet:

- Entfernen des Access-Codes: 0112 -> 112
- Einfügen von <LDAP-Belegungskennzahl><InternationalesPräfix><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.

Tip: 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

Richtungsparameter

Knoten 4, Telefone

Übersicht der für einen Notruf relevanten Einträge im LCR 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

Richtung	Nr-Typ, gehend	RNR-Typ
Vernetzung	National	Int/Duwa

Richtung Networking	
Amtskennziffer (2. AKZ)	0

Standort Witten	
Rufnummer	1101
Emergency Number (Notrufnummer)	4923026670

Standort München	
Rufnummer	2101
Emergency Number (Notrufnummer)	49897220

Standort Paderborn	
Rufnummer	3102
Emergency Number (Notrufnummer)	49525180

Anruf-Routing

Anrufsteuerungsdienst (Call Admission Control)

Standort Augsburg	
Rufnummer	4102
Emergency Number (Notrufnummer)	490

Rufnummernplan		Wegetabelle			Wahlregel			
Name	Gewählte Ziffern	Not- betrieb	Richtung	Dediziertes Gateway	Gateway ID	Wahlregel	Verfahren	Typ
Notruf ⁵	0C112	X	Vernetzung	Multi-Gateway	1	E1A	Corp. Network	Unbekannt
Notruf ⁵	0C0110	X						
Amt	0CZ							
Notruf_nach1	0C00492302667-0-11X	X	Vernetzung	Erzwungen	1	E3A	Corp. Network	Unbekannt
Notruf_nach2	0C004989722-0-11X	X			2			
Notruf_nach3	0C004952518-0-11X	X			3			
Notruf_4lokal ⁶	0C0049-0-11X	X	ITSP	Nein		E4A	Hauptnetzanbieter	Unbekannt

15.4.5 Notrufdienst E112 (für Europa)

Durch den erweiterten Notrufdienst E112 werden neben der Rufnummer auch Informationen über den geographischen Standort (hinterlegte Adresse) des Anrufers beim Absetzen eines Notrufs übermittelt.

Die geografischen Informationen werden in einem standardisierten XML-Dokument übertragen. Die inhaltliche Definition dieses Dokuments variiert je nach Land und ITSP. Sie müssen daher nur die Teilmenge an Daten eingeben, die Sie von Ihrem ITSP erhalten haben (z. B. in der Schweiz nur den NAM-Parameterwert).

Das Leistungsmerkmal wird durch Einrichtung von Notrufnummern in der LCR-Konfiguration und Angabe von geeigneten Standortinformationen aktiviert.

15.5 Anrufsteuerungsdienst (Call Admission Control)

Über das Leistungsmerkmal Anrufsteuerungsdienst (Call Admission Control CAC) kann die benutzte Bandbreite über die Anzahl von Gesprächen eingeschränkt werden.

Das Kommunikationssystem bietet drei Möglichkeiten Einfluß auf die benötigte Bandbreite zu nehmen:

⁵ Mit den obigen Regeln wird in diesem Beispiel nur die Notrufsituation erkannt, aber nicht geroutet. Für das Notruf-Routing wird die abgeleitete "lange" Notrufnummer verwendet.

⁶ Weil am Multi-Gateway-Standort Teilnehmer physikalisch angeschlossen sind, ist eine eigene LCR-Regel für einen lokalen Notrufzugang einzutragen (via ITSP-Richtung).

- Einschränkung der Anzahl gleichzeitiger 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 maximal mögliche Anzahl von Anrufen über ITSP festgelegt. Durch Herabsetzen der Anzahl dieser Anrufe (Internet-Anrufe) 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.

Internet-Anrufe sind:

- ITSP-Anrufe
- myPortal@work-Anrufe
- Device@Home-Anrufe
- Circuit-Anrufe

Nur bei LAN myPortal@Work und PureWebRTC-Anrufen wird keine Bandbreite reserviert, da die Nutzdaten direkt sind.

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 Vernetzungsszenarien

Das Kommunikationssystem bietet zwei Möglichkeiten die Bandbreite in Vernetzungsszenarien zu kontrollieren.

Beschränkung durch die Anzahl der Leitungen zu anderen Netzknotten

Beschränkung der Bandbreite durch gezielte Codec-Auswahl

Durch Zuordnung einer bestimmten Anzahl von Leitungen zu anderen Netzknotten kann eine Obergrenze aller gleichzeitig möglichen Gespräche von und zu diesen Knoten vorgenommen werden.

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 Untereinheiten 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 Anrufe
- Internes Verzeichnis
- KDS-Ausdruck
- Nachtschaltung
- Parkposition
- Verkehrsbeziehungsgruppen
- Voicemail
- Amtsberechtigung

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 Anrufe	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 Verzeichnis	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 zugewiesen 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	OpenScape Business X OpenScape Business S	Erforderlich
Company AutoAttendant (UC Suite)	UC Suite	OpenScape Business X3/ X5/X8 mit UC Booster Card oder UC Booster Server OpenScape Business S	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	
myAttendant	UC Suite	OpenScape Business X3/ X5/X8 mit UC Booster Card oder UC Booster Server OpenScape Business S	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.

Anmerkung: Um einen automatischen Abwurf zum Vermittlungsplatz durch das Voicemailsysteem zu gewährleisten ist zwingend die Platzkennzahl intern einzutragen (Default 9, USA 0).

Anmerkung: 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!

Anwendungsfälle

- 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 die Option, 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 AutoAttendant 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.

16.1.2 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

Dieser Zeitplan und die darin enthaltenen Regeln (Call Control Vector CCV) definieren, 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.

Anmerkung: Eine Regel hat eine Obergrenze von 500 CCV-Objekten.

Folgende vordefinierte CCV-Objekte stehen zur Verfügung:

Tipp: 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 andere 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 möglich, eine Audio-Datei im wav-Format direkt 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**

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 Ziffern mit Ziel.

Die Ziffern und Ziele können hinzugefügt, bearbeitet und entfernt werden.

- **Datei-Manager:** Über diese Schaltfläche ist es möglich, eine Audio-Datei im wav-Format direkt 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.

Tipp: 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 die Übergabe des Anrufs wenn das Zeil 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.

Anmerkung: Nach einer Einzelschritt-Übergabe trennt das System die Verbindung nach Klingeln für 5 Minuten.

- **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 (Supervised Transfer)**

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 sowie externe CallMe-Ziele ist nicht zulässig! Für diese Szenarien ist der SST (Einzelschritt Übergabe) zu verwenden.

- **Zeitüberschreitung beim Klingeln (Sek.):** 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.

Tipp: Die hier angegebene Zeit muss kürzer sein als die für die Rufweiserschaltung konfigurierte Zeit (Standardeinstellung für die Rufweiserschaltung = 15 Sekunden). Siehe [Rufweiserschaltung konfigurieren](#).

- **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 Anrufweiserschaltung oder Anrufumleitung aktiviert, wird der Anruf zum Kommunikationssystem zurückgestellt und das nächste CCV-Objekt verwendet.

- **Anwesenheitsstatus bei Anrufübergabe prüfen:** Option

Bei aktivierter Option erfolgt eine Prüfung des Anwesenheitsstatus des Anrufziels. Bei einem anderen Anwesenheitsstatus als Büro wird der Anruf zum Kommunikationssystem zurückgestellt und das nächste CCV-Objekt verwendet.

Anmerkung: Wenn ein eingehender Anruf von einer unterdrückten/unbekannten Nummer kommt und der Anruf vom UC Suite AutoAttendant angenommen und über die überwachte

Übertragung weitergeleitet wird, wird als Nummer des Anrufers die UC Suite-Nummer angezeigt.

- **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.

Tipp: 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 +49 eine deutsche Ansage und für eine Rufnummer mit der Ländervorwahl +33 eine französische Ansage abgespielt wird.

Eigenschaften:

- **Standardsprache:** 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 den zugehörigen (dem **Muster** entsprechenden) Rufnummern zugeordnet werden soll.

Eine Sprache kann beliebig vielen verschiedenen (dem **Muster** entsprechenden) Rufnummern 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 +49 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**). Es kann auch die Ortsvorwahl verwendet werden (z B. 089 für München).

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 Rufnummern, denen 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** +49 (=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 den zugehörigen (dem **Muster** entsprechenden) Rufnummern als Ziel zugeordnet werden soll.

Beliebig vielen verschiedenen (dem **Muster** entsprechenden) Rufnummern 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:

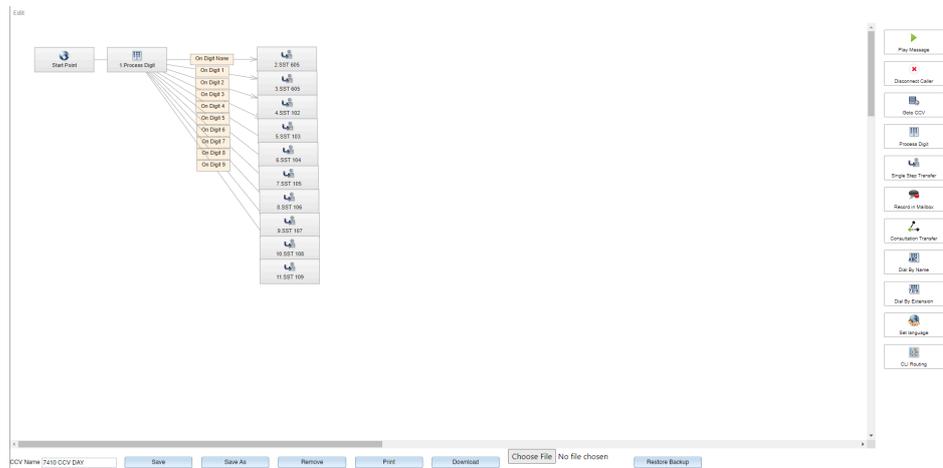
- Agent im Zustand "Klingeln"
- Agent im Zustand 'Gespräch'
- Agent in Zustand "Nachbearbeitung"
- Agent im Zustand "Verpasster Anruf"
- Agent im Zustand "Überfällig"

16.1.2.2 Vorlagen (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.

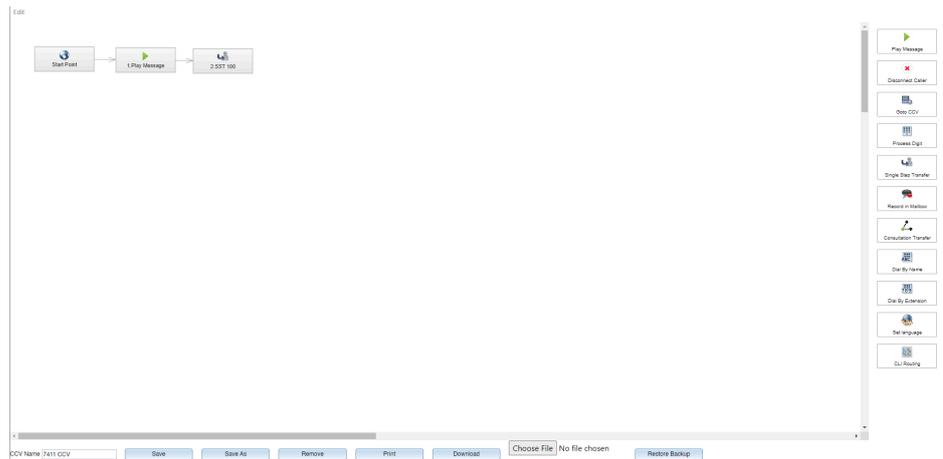
Vorlage 1 – 7410 CCV: Anruf mit Durchschaltung (ohne Mailbox)

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.



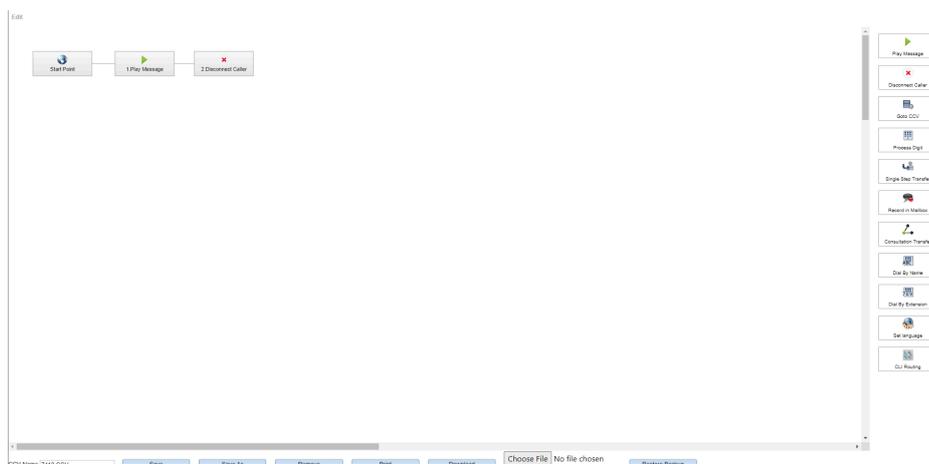
Vorlage 2 – 7411 CCV: Ansage vor Beantwortung

Dem Anrufer wird eine Ansage vorgespielt. Anschließend wird auf den Abwurfplatz 100 vermittelt.



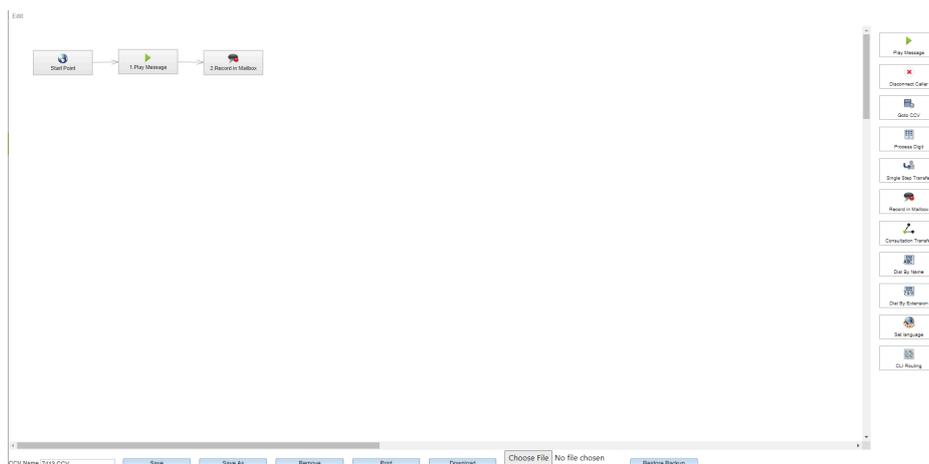
Vorlage 3 – 7412 CCV: Anruf außerhalb der Geschäftszeit

Dem Anrufer wird bei einem eingehenden Anruf außerhalb der Geschäftszeiten eine Ansage vorgespielt. Anschließend wird die Verbindung getrennt.



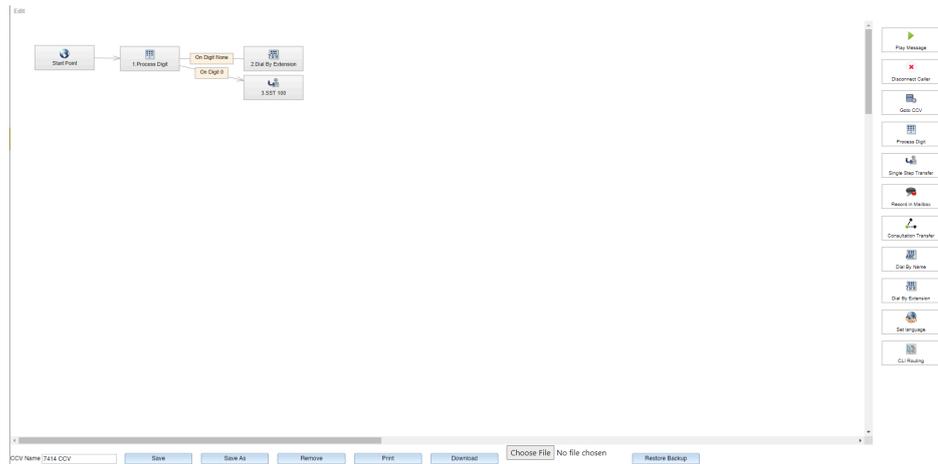
Vorlage 4 – 7413 CCV: 7413 CCV: Anruf außerhalb der Geschäftszeit mit Rufweitschaltung auf eine Mailbox

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.



Vorlage 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.

Weitere Information

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 / Live Recording
- Benachrichtigungsruf (SMS und Pager möglich)
- Weiterleitung von Nachrichten per Namenswahl
- Weiterleiten von Faxanrufen
- Statistiken für Vermittlungsmailboxen
- Zentrale Voice-Mailbox
- Zugangsschutz (3- bis 8-stelliges Passwort)

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.

Tastenlayout

Am OpenStage Attendant kommen alle Gespräche an, für die keine Durchwahlmöglichkeit besteht, oder für die über die Rufzuordnungskriterien 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

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 in einem Netzwerk erweitert werden, um netzweite BLF- und Anwesenheitsinformationen anzuzeigen.

Attendants

The screenshot shows the Attendant software interface. At the top, there is a navigation bar with buttons for Consultation, Toggle, Consultation back, Transfer, and Disconnect. The title bar reads 'Attendant' and includes standard window controls. Below the navigation bar is a status area with a 'Status' icon and a text input field for 'Enter phone number / name-->' with a 'Help' button.

The main area is divided into sections: 'Incoming calls' and 'Parked / Holded conversations'. Below this is a section for 'Active:' and 'Passive:' calls. A menu bar includes 'BLF', 'Telephone book', 'List of callers', and 'Voicemail'.

The central part of the interface is a grid of employee stations, organized into columns for different office floors and departments. The stations are as follows:

Office 1.Floor	Office 2.Floor	Office 3. Floor		
100 John Smith	+ 104 Pierre Martin	106 Christophe Lambe		
101 Janet Jones	105 Natalie Dubois	107 Flor Peeters		
102 Susanne Mueller		108 Giovani Rossi		
		109 Angelina Mancini		
Support	Labor	Sales		Features
110 Maria Sanchez	114 Anna Nowak	116 James Campbell		Override busy station
111 Julio Gomez	115 Jan Kowalski	117 Morag Reid		Activate night answer
112 Danny De Jong		118 Buddy Miller		Mute on/off
113 Antje Janssen		119 Akiko Watanabe		Display suppression
		120 Kim Chang		Hold
130 FAX		103 Manfred Schmitz		Park
		199 FAX		Call

At the bottom of the interface, there is a status bar that reads 'Ready to operate' and a system tray with a 'T' icon and a help icon.

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 Verzeichnis

Besetztlampenfeld-Status:

- Frei, Besetzt, Gerufen, Umgeleitet

Sichtbarkeit Präsenzstatus:

- Büro, Besprechung, Krank, Pause, Außer Haus, Urlaub, Mittagspause, Zuhause

Anmerkung: Der Anwesenheitsstatus "krank" ist je nach Systemeinstellung des Administrators möglicherweise nicht verfügbar.

- Ändern des Anwesenheitsstatus für Teilnehmer des eigenen Knotens (derzeit nicht für Teilnehmer aus anderen Knoten)

Für die Darstellung der Benutzeroberfläche von OpenScape Business Attendant stehen zwei unterschiedliche Styles zur Verfügung.

Es können maximal acht OpenScape Business Attendants je Kommunikationssystem angeschlossen werden (maximal acht Lizenzen je OpenScape BusinessX1/X3/X5/X8 und Business OpenScape BusinessS).

Die Lizenzierung des OpenScape Business Attendant geschieht über das WBM.

Technische Voraussetzungen

- Standard Windows-PC
- Möglicher Einsatz eines Terminal Servers bei Verwendung von HFA-Telefonen (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 16 Bit Farbtiefe (min. 256 Farben)
- Internetzugang für Support bzw. Updates

Betriebssystem

- Microsoft Windows 10 / 8.1 / 8 / 7 (jeweils als 32 Bit oder 64 Bit möglich)
- Microsoft Windows Vista (32 Bit)
- Microsoft Windows Server 2015 (32 Bit / 64 Bit) als Microsoft Terminal Server
- Microsoft Windows Server 2012 (32 Bit / 64 Bit) als Microsoft Terminal Server

- Microsoft Windows Server 2008 R2 (64 Bit) als Microsoft Terminal Server

Der Support von OpenScape Business Attendant für Microsoft Windows XP und Microsoft Windows Server 2003 endet zeitgleich mit der Einstellung des Produktsupports durch Microsoft. Das Produkt wird weiterhin unterstützt, jedoch nicht mehr detailliert getestet.

Unterstützte Telefone

- OpenStage 40/60/80 HFA
- OpenStage 30T/40T/60T/80T
- OpenScape DeskPhone CP 100/200/205/400/600/600E/700/700X
- OpenScape DeskPhone CP 110/210/710

Anmerkung: Beim OpenScape DeskPhone CP 200/205/210 wird bei einem externen Anruf der Name des Benutzers nicht angezeigt.

Ältere Geräte (z. B. optiPoint410/420/500) werden teilweise noch unterstützt. Getestete und freigegebene Geräte entnehmen Sie bitte den jeweiligen Freigabemitteilungen.

Einfaches Plug-and-Play bei der Installation

Der OpenScape Business Attendant wird bei der Ersteinrichtung über einen Wizard konfiguriert. Der Wizard öffnet die erforderlichen Konfigurationsdialoge.

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 Besetztlampenfeld OpenScape Business BLF ist eine eigenständige Applikation zur Anzeige von Belegzuständen. Optionale Funktionen sind Anzeige und Setzen des Anwesenheitsstatus, sowie der Verbindungsaufbau für das zugeordnete Telefon.

Technische Voraussetzungen

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

Zum Betrieb des OpenScape Business BLF ist eine OpenScape Business BLF-Lizenz plus eine UC User-Lizenz erforderlich.

- Standard Windows-PC
- Microsoft Windows 10 / 8.1 / 8 / 7 (jeweils als 32 Bit oder 64 Bit möglich)
- Microsoft Windows Vista (32 Bit)
- Microsoft Windows Server 2015 (32 Bit / 64 Bit) als Microsoft Terminal Server
- Microsoft Windows Server 2012 (32 Bit / 64 Bit) als Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 (64 Bit) als Microsoft Terminal Server
- Bildschirm mit einer Auflösung von min. 1024x768
- Grafikkarte mit 16 Bit Farbtiefe (min. 256 Farben)
- LAN-Schnittstelle
- Standard Maus und Tastatur
- Internetzugang für Support bzw. Updates

16.3.2 Einrichteispiele für OpenScape Business Attendant, OpenScape Business BLF

In den folgenden Kapiteln finden Sie Einrichteispiele für die generelle Konfiguration von OpenScape Business Attendant, OpenScape Business BLF.

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.

Wesentliche Vermittlungsfunktionen

Pro Kommunikationssystem (pro Netzknoten) können maximal 20 myAttendant angeschlossen werden. Der Maximalausbau eines Netzverbands 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.

- Anstehende bzw. angenommene Anrufe verwalten
- Daten des aktiven Gesprächs werden angezeigt
- Geparkte, gehaltene Gespräche werden angezeigt
- Anruferliste

Attendants

- 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)

Anmerkung: Der Anwesenheitsstatus "krank" ist je nach Systemeinstellung des Administrators möglicherweise nicht verfügbar.

- 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 Vertriebsinformation)

- Standard Windows-PC
- Microsoft Windows 10 / 8.1 / 8 / 7 (jeweils als 32 Bit oder 64 Bit möglich)
- Microsoft Windows Vista (32 Bit)
- Terminal Server Einsatz möglich

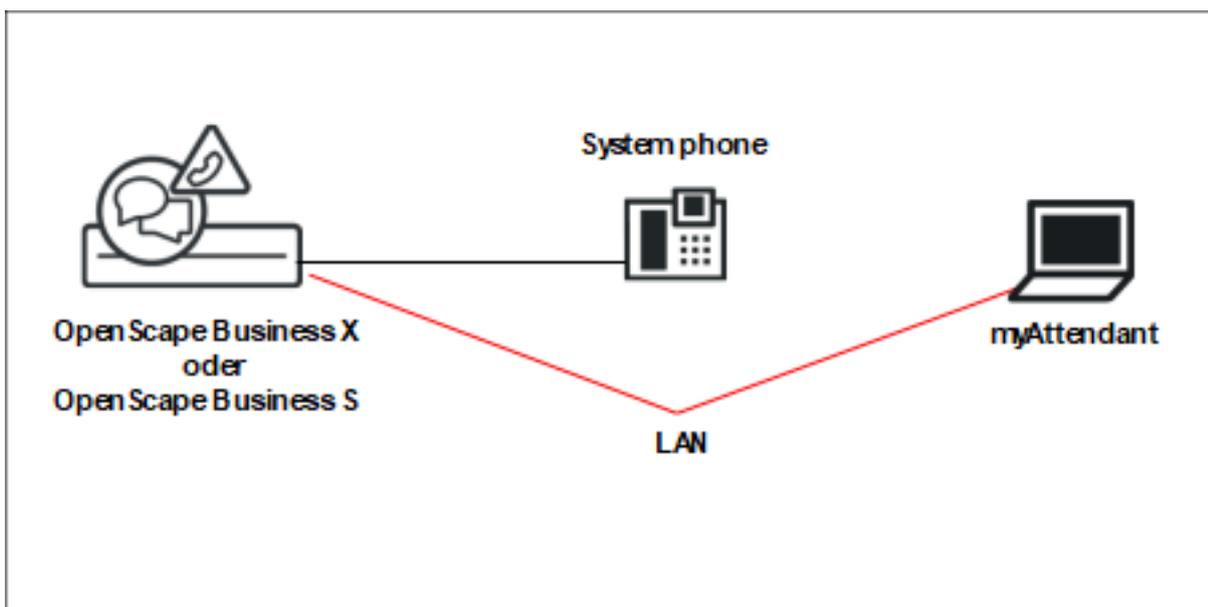
Zusätzliche Software

- Auf einem PC muss Oracle Java Version 8 oder höher bzw. OpenJDK 8 installiert sein (siehe **Service-Center > Software**)

Unterstützte Telefone

- OpenStage 40/60/80 HFA
- OpenScape Desk Phone IP 35G/55G HFA
- OpenScape Desk Phone IP 35G Eco HFA
- OpenScape Desk Phone CP 100/200/205/400/600/600E/700/700X HFA
- OpenScape Desk Phone CP 110/210/710 HFA
- SIP-Telefone mit RFC 3725-Unterstützung, z. B. OpenScape Desk Phone IP 35G/55G SIP, OpenScape Desk Phone CP 100/200/205/400/600/600E/700/700X SIP, OpenScape Desk Phone CP 110/210/710 SIP
- OpenStage 30T/40T/60T/80T

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 100 Benutzerschaltflächen zur Verfügung. Sie können die Standardanzahl der Benutzerschaltflächen pro Registerkarte jederzeit ändern.

Die Benutzerschaltflächen sind standardmäßig alphabetisch nach Nachname sortiert.

Es können mehrere Registerkarten für Benutzerschaltflächen eingerichtet werden; für diese Benutzerschaltflächen können Sie die Namen frei wählen.

Den Benutzerschaltflächen können interne, externe und persönliche Kontakte (Benutzer) zugeordnet werden.

16.4.2 Nachrichtencenter

Im **Nachrichten-Center** von myAttendant werden Sprach-, Fax- und Sofornnachrichten, 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 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.

16.5 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
- MULAP-Gruppe
- 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 (2-stellig) 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 Rufweitschaltung). Nimmt kein Teilnehmer den Anruf an, wird er zum Abwurfplatz weitergeleitet.
- Im Besetztfall, falls keine Weitschaltung 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 Rufweitschaltung). 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 Rufweitschaltung). Nimmt kein Teilnehmer den Anruf an, wird er zum Abwurfplatz weitergeleitet.
- Bei fehlender Rufnummer
Wie bei Falschwahl.
- Bei Anrufweitschaltung mit Verkettung
Wenn ein umgeleiteter Anruf am Ziel der Umleitung jeweils auf eine weitere Anrufumleitung trifft und dabei die Anzahl der zulässigen Verkettungen überschritten wird, erfolgt Abwurf. Die Anzahl der zulässigen Verkettungen ist abhängig von den Eintragungen in der Rufweitschaltung, maximal sind drei Verkettungen erlaubt.
- Bei Codeschloss

Attendants

Wählt ein Teilnehmer an einem Telefon mit aktiviertem Codeschloss eine Richtungskennzahl, erfolgt Abwurf. Für diesen Fall legt der Administrator ein separates Abwurfziel fest.

- Bei Ansage (nur mit UC Suite)

Wählt ein Teilnehmer die Platzkennzahl (2-stellig), während er eine Ansage der Sprachbox oder des AutoAttendant hört, erfolgt Abwurf. Für diesen Fall legt der Administrator ein separates Abwurfziel fest.

Abhängigkeiten

Themenbereich	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.
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 vergebene 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.

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.

Tipp: 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 Nachbearbeitungscodes des Contact Centers erstellt werden. Mehr als 100 vordefinierte Berichtsvorlagen stehen zur Verfügung.

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
 - Faxe
 - 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
 - Anrufüberwachung (länderabhängig)
 - Aufschalten auf Anrufe
 - Sofortnachricht versenden
- 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 [Berechtigungsunabhängige Funktionen für Agenten](#)).

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 in Warteschlange**

Anrufe, die diese Wartezeit überschreiten, erhält ein Agent bei Überlauf.

- **Überlauf nach Anrufen in Warteschlange**

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 nutzen zu können, muss der Client-PC des Teilnehmers eine geeignete Hardware- und Softwareausstattung haben.

Tipp: 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
- OpenScape Desk Phone IP 35G Eco HFA
- OpenScape Desk Phone CP 100/200/205/400/600/600E/700/700X HFA
- OpenScape Desk Phone CP 110/210/710 HFA
- OpenStage T
- OpenScape Personal Edition HFA
- OpenStage M3 (OpenScape Business Cordless)

- OpenScape DECT Phone S6/SL6/R6 (OpenScape Business Cordless)

Ältere Geräte (z. B. optiPoint 410/420/500 und Gigaset M2/SL3/S4/SL4/S5) werden unterstützt. Optiset E-Geräte können nicht betrieben werden. 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.

Betriebssysteme

myAgent kann in Verbindung mit folgenden Betriebssystemen verwendet werden:

- Microsoft Windows 10 / 8.1 / 8 / 7 (jeweils als 32 Bit oder 64 Bit möglich)
- Microsoft Windows Vista (32 Bit)

Tipp: 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 Server 2003 endet zeitgleich mit der Betreuungseinstellung durch Microsoft. Das Produkt wird weiterhin unterstützt, jedoch nicht mehr detailliert getestet.

Zusätzliche Software

- Auf einem PC muss Oracle Java Version 8 oder höher bzw. OpenJDK 8 installiert sein (siehe **Service-Center > Software**)
- Adobe Reader 9 oder höher (für Berichte im PDF-Format)

Hardware Mindestanforderungen

- 2 GHz CPU
- RAM: 2 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:

Tipp: Terminalserver- und Citrix-Server-Umgebungen inklusive Hosted Services und virtuelle Umgebungen liegen in der Verantwortung des Kunden.

Tipp: Citrix-Server-Umgebungen können einige regionale Buchstaben (z. B. deutsche Umlaute) nicht korrekt decodieren.

Betriebssysteme:

- Microsoft Windows Server 2015 (32 Bit / 64 Bit) als Microsoft Terminal Server
- Microsoft Windows Server 2012 (32 Bit / 64 Bit) als Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 (64 Bit) als Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 (64 Bit) mit Citrix XenApp 6.5 Server (Desktop Mode)

Der Support von myAgent für Microsoft Windows XP und Microsoft Windows Server 2003 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 von der Server-Performance und dem zur Verfügung stehenden Arbeitsspeicher ab. 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.

Beachten Sie die Hinweise in der Datei *ReadMe first*, die sich im Ablageverzeichnis der Installationsdateien befindet.

Tipp: Die automatische Verteilung der MSI-Datei über einen Deployment-Dienst 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

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: Aktivität	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
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		
Sprache der Benutzeroberfläche ändern	X	X
Farbe der Benutzeroberfläche ändern	X	X
E-Mail-Vorlage konfigurieren	X ⁷	X
Serveradresse ändern	X	X
Administrator-Kennwort ändern		X

⁷ Für die Konfiguration der E-Mail-Vorlage ist die Eingabe des Administrator-Kennworts erforderlich.

myReports: Aktivität	Benutzerrolle	
	myReports Benutzer	myReports Administrator
Vorwahlen für externe Rufnummern konfigurieren		X
Datenschutz aktivieren/ deaktivieren		X
Speicherort für den Export zeitgesteuerter Berichte konfigurieren		X
Sprache einrichten		X ⁸
Standard-Sprache einrichten		X ⁸

17.1.4 Voraussetzungen für myReports

Um myReports zu nutzen, muss der Client-PC des Teilnehmers über eine geeignete Hardware- und Softwareausstattung verfügen.

Tipp: Beachten Sie bitte unbedingt die Hinweise in der Datei `ReadMe first`, die sich im Ablageverzeichnis der Installationsdateien befindet.

Betriebssysteme

myReports kann in Verbindung mit folgenden Betriebssystemen verwendet werden:

- Microsoft Windows 10 / 8.1 / 8 / 7 (jeweils als 32 Bit oder 64 Bit möglich)
- Microsoft Windows Vista (32 Bit)

Tipp: 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 Server 2003 endet zeitgleich mit der Betreuungseinstellung durch Microsoft. Das Produkt wird weiterhin unterstützt, jedoch nicht mehr detailliert getestet.

Zusätzliche Software

- Auf einem PC muss Oracle Java Version 8 oder höher bzw. OpenJDK 8 installiert sein (siehe **Service-Center > Software**)

⁸ Für die Einrichtung der Sprache und der Standard-Sprache ist die Anmeldung als myReports-Administrator mit einem speziellen Kennwort erforderlich.

- Adobe Reader 9 oder höher (für Berichte im PDF-Format)
- Microsoft Excel 16 / 2013 / 2010 (für Berichte im Excel-Format)
- Microsoft Word 16 / 2013 / 2010 (für Berichte im Word-Format)

Hardware Mindestanforderungen

- 2 GHz CPU
- RAM: 2 GB
- 100 Mbit/s LAN (1 Gbit/s LAN empfohlen)
- XGA (1024x768) Bildschirmauflösung, myPortal for Outlook: SVGA (800x600) Bildschirmauflösung

Multi-User 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.

Tipp: Terminalserver- und Citrix-Server-Umgebungen inklusive Hosted Services und virtuelle Umgebungen liegen in der Verantwortung des Kunden.

Tipp: Citrix-Server-Umgebungen können einige regionale Buchstaben (z. B. deutsche Umlaute) nicht korrekt decodieren.

Betriebssysteme:

- Microsoft Windows Server 2015 (32 Bit / 64 Bit) als Microsoft Terminal Server
- Microsoft Windows Server 2012 (32 Bit / 64 Bit) als Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 (64 Bit) als Microsoft Terminal Server
- Microsoft Windows Server 2008 R2 (64 Bit) mit Citrix XenApp 6.5 Server (Desktop Mode)

Hardware-Voraussetzungen: Die Anzahl der installierbaren Clients hängt von der Server-Performance und dem zur Verfügung stehenden Arbeitsspeicher ab. 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.

Beachten Sie die Hinweise in der Datei `ReadMe first`, die sich im Ablageverzeichnis der Installationsdateien befindet.

Tipp: Die automatische Verteilung der MSI-Datei über einen Deployment-Dienst 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 @work und myPortal to go verwendet.

Beispiele gegenseitiger Beeinflussung:

- Änderung des Anwesenheitsstatus über myPortal

Die Beispiele gelten für die Standardeinstellung **Sprachnachrichten** (Voicemail) 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 [Berechtigungsabhängige Funktionen für Agenten](#)).

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 ein Administrator verfügt über erweiterte Berechtigungen.

Die Unterschiede zwischen den Berechtigungs-Levels sind in der folgenden Tabelle zusammengefasst.

myAgent: Aktivität	Berechtigungs-Level		
	Agent	Supervisor	Administrator
Agent einer Warteschlange zuordnen	-	X	X
Agent zu anderer Warteschlange verschieben	-	X	X
Agent aus Warteschlange entfernen	-	X	X
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 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
Call Supervision (länderabhängig)	-	X	X
Wie Sie sich auf einen 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.

17.2.5 An- und Abmeldung des Agenten per Telefon

Anmeldung/Abmeldung beim Contact Center wird auch über Telefon unterstützt; dabei besteht keine Notwendigkeit zur Ausführung von myAgent, um die Contact Center-Funktionen nutzen zu können. Wenn ein Agent über Telefon angemeldet wurde, können nur Sprachanrufe verarbeitet werden. Popup-Fenster und die Eingabe von Nachbearbeitungscodes werden in diesem Fall nicht unterstützt. Dies gilt auch, wenn der Agent sich bei aktivem myAgent über Telefon beim Contact Center anmeldet. Um die volle Funktionalität von myAgent wiederherzustellen, muss der Agent sich über Telefon abmelden und anschließend über myAgent wieder anmelden.

Voraussetzungen und Einschränkungen

- OpenScape Business Contact Center Leistungsmerkmale funktionieren über Telefon nur für Agenten, denen in OpenScape Business eine myAgent-Lizenz zugeordnet ist
- Alle Funktionen werden nur auf Telefonen unterstützt, die für die Verwendung mit OpenScape Business Contact Center freigegeben sind

- Wenn die Anmeldung über Telefon erfolgreich war und der zugehörige myAgent-Client nicht aktiv ist, werden nur Sprachanrufe an den Agenten weitergeleitet
- Wenn die Anmeldung über Telefon erfolgreich war und der zugehörige myAgent-Client aktiv ist, werden E-Mails/Faxe und Rückrufe nicht an den Agenten weitergeleitet, wenn dieser über Telefon angemeldet ist. In diesem Fall funktionieren Pop-up-Fenster und Nachbearbeitung wie gewohnt, aber nur Sprachanrufe werden an den Agenten weitergeleitet. Um die volle Funktionalität wiederherzustellen, muss sich der Agent zunächst über Telefon abmelden und dann erneut über myAgent anmelden

Anmeldung über Telefon beim Contact Center

Wenn die Agenten sich beim OpenScape Business Contact Center über Telefon anmelden (unabhängig davon, ob der myAgent-Client und das Contact Center aktiv ist):

- Am Telefon werden die UCD-Funktionen für die Anmeldung verwendet
- Die Anmeldung kann entweder per Leistungsmerkmal-Code oder über eine programmierte Taste erfolgen
- Der Agent wird bei allen Warteschlangen angemeldet, denen er innerhalb der Contact Center-Konfiguration zugeordnet ist
- Am Telefondisplay wird der Anmeldestatus des Agenten angezeigt
- Bei Bedarf können nur die UCD-Warteschlangeninformationen (z. B. Informationen zu Anrufen in der Warteschlange) angezeigt werden

Der Agent kann folgende Funktionen verwenden:

- Anmeldung/Abmeldung (mit UCD Agenten-ID)
- Nachbearbeitung
- Verfügbar/Nicht verfügbar
- Anzeige der in der UCD-Warteschlange eingereichten Anrufe mit zugeordneter UCD-Agenten-ID

Anmerkung: Die UCD-Nachtschaltung darf nicht vom Agenten verwendet werden.

Anmerkung: Das Flag für „myAgent permanent verfügbar“ wird für die Anmeldung über das Telefon unterstützt. Das bedeutet, dass, wenn ein Agent mit seinem Telefon angemeldet ist und ein Anruf verpasst wurde, dieser Agent für den nächsten Anruf verfügbar bleibt. Dies ist das gleiche Verhalten wie bei der Verwendung des myAgent Client.

Fällt das Contact Center aus, während der Agent angemeldet ist, bleibt der Agent bei UCD angemeldet und Sprachanrufe werden entsprechend der UCD-Routing-Konfiguration weitergeleitet. Wenn der Agent nicht angemeldet war, kann er sich über Telefon bei UCD anmelden.

Abmeldung über Telefon beim Contact Center

Wenn die Agenten sich beim OpenScape Business Contact Center über Telefon abmelden (unabhängig davon, ob der myAgent-Client und das Contact Center aktiv ist):

- Am Telefon werden die UCD-Funktionen für die Abmeldung verwendet
- Die Abmeldung kann entweder per Leistungsmerkmal-Code oder über eine programmierte Taste erfolgen
- Der Agent wird bei allen Warteschlangen abgemeldet, denen er innerhalb der Contact Center-Konfiguration zugeordnet ist
- Am Telefondisplay wird der Abmeldestatus des Agenten angezeigt
- Zusätzliche Contact Center / UC-Informationen (z.B. Informationen zu Anrufen in der Warteschlange) werden nicht angezeigt

Agent per Telefon als verfügbar/nicht verfügbar einstellen

Wenn ein Agent seinen Status für OpenScape Business Contact Center Kontakttrouing über Telefon auf Verfügbar / Nicht Verfügbar setzt (unabhängig davon, ob der myAgent-Client und das Contact Center aktiv ist):

- Am Telefondisplay wird der Anmeldestatus des Agenten angezeigt
- Wenn myAgent nicht aktiv ist, werden nur Sprachanrufe an den Agenten weitergeleitet

Bearbeitung nach Anruf (Nachbearbeitung) über Telefon setzen/rücksetzen

Wenn ein Agent seinen Status über Telefon auf "Bearbeiten nach Anruf" (Nachbearbeitung) setzt (unabhängig davon, ob der myAgent-Client und das Contact Center aktiv ist), werden keine Anrufe zum Agenten weitergeleitet, bis die im OpenScape Contact Center konfigurierte Nachbearbeitungszeit des Agenten abgelaufen ist oder der Agent die Nachbearbeitung über Telefon zurückgesetzt hat.

Statuszuordnung

Über Telefon geänderte Agentenstatus werden myAgent-Agentenstatus wie folgt zugeordnet:

Telefongerät			myAgent			
Leistungs Code	Leistungs Code	Beschreibung	Telefondisp	Status	Zusatztext	Bemerkung
*401	UCD Agenten-ID	UCD-Agenten einloggen	Verfügbar	Verfügbar	-	Der Status des Agenten wird in allen zugeordneten Warteschlangen auf "Verfügbar" gesetzt

Telefongerät			myAgent			
Leistungs Code	Leistungs Code	Beschreibung	Telefondisp	Status	Zusatztext	Bemerkung
#401	-	UCD-Agenten ausloggen	Nicht verfügbar	Nicht verfügbar	-	Der Status des Agenten wird in allen zugeordneten Warteschlangen auf "Nicht verfügbar" gesetzt
*402	-	UCD-Agent verfügbar	Verfügbar	-	-	Verfügbar (Ende der Nachbearbeitung)
#402	-	UCD-Agent nicht verfügbar	Nicht verfügbar	Nachbearbeitung	Countdown von 999.999 Sekunden	-
*403	-	UCD-Nachbearbeitung ein	Nachbearbeitung	Nachbearbeitung	Countdown der konfigurierten Nachbearbeitungszeit	Die Nachbearbeitung muss abgeschlossen sein, bevor sie erneut gestartet werden kann. Eine Kumulierung der Nachbearbeitungszeit wie bei myAgent gibt es nicht. Nach Ablauf der Nachbearbeitungszeit wird der Agentenstatus automatisch auf Verfügbar gesetzt.
#403	-	UCD-Nachbearbeitung aus	Verfügbar	Verfügbar	-	-
*404	Nachtschaltung Ziel	UCD-Nachtschaltung ein	-	Nicht unterstützt	-	UCD-Nachtschaltung darf nicht verwendet werden

Telefongerät		myAgent				
Leistungs Code	Leistungs Code	Beschreibung	Telefondisp	Status	Zusatztext	Bemerkung
#404	-	UCD-Nachtschaltung aus	-	Nicht unterstützt	-	UCD-Nachtschaltung darf nicht verwendet werden
*405	-	UCD-Rufqueue-Status abfragen	-	-	-	Nur die Warteschlange mit zugeordneter UCD-Agenten-ID wird angezeigt, unabhängig davon, ob der Agent mehreren Warteschlangen im Contact Center zugeordnet ist

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

Sie haben die folgenden 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

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.

- Warteschlangen-Tiefe konfigurieren

Kontrolle über die maximale Anzahl von aktiven und wartenden Anrufen in einer bestimmten Warteschlange. Das Contact Center weist das System darauf hin, wenn der definierte Schwellwert für die Warteschlangengröße erreicht ist. In der Folge weist das System jeden neuen bei der entsprechenden Warteschlange eingehenden Anruf zurück, bevor dieser mit dem System verbunden wird; dies geschieht solange, bis die Anzahl der Anrufe unter den Schwellwert fällt.

Die maximale Warteschlangengröße hängt von folgenden Parametern ab:

- Maximale Anzahl an Wartepositionen in der Warteschlange. (WLS = Waiting Loop Size, Warteschlangengröße)
- Maximale Anzahl aktiver und wartender Anrufe in der Warteschlange. (Warteschlangentiefe-Größe).
- 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 definiert werden, wie kommende Anrufe beispielsweise während der Urlaubszeit behandelt werden sollen. Urlaubspläne haben 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.

Anmerkung: Eine Regel hat eine Obergrenze von 500 CCV-Objekten.

Folgende vordefinierte CCV-Objekte stehen zur Verfügung:

Tipp: 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 andere 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 möglich, eine Audio-Datei im wav-Format direkt 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

- **Geschätzte Wartezeit**

Bewirkt die Information des Anrufers über seine geschätzte Wartezeit.

Die Berechnung der geschätzten Wartezeit erfolgt auf der Grundlage von:

- 1) Durchschnittliche Wartezeit in allen Warteschlangen in der Vergangenheit
- 2) Durchschnittliche Wartezeit in einer bestimmten Warteschlange in der Vergangenheit
- 3) Durchschnittliche Gesprächszeit für den bestimmten Agent in der Vergangenheit

- **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 dem 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**

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 (Ansprache) erneut abgespielt.

- **Link an:** Auflistung der Ziffern mit Ziel.

Die Ziffern und Ziele können hinzugefügt, bearbeitet und entfernt werden.

- **Datei-Manager:** Über diese Schaltfläche ist es möglich, eine Audio-Datei im wav-Format direkt 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.

Tipp: 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 die Übergabe des Anrufs wenn das Zeil 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.

Anmerkung: Nach einer Einzelschritt-Übergabe trennt das System die Verbindung nach Klingeln für 5 Minuten.

- **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 (Supervised Transfer)**

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.

Tipp: Die hier angegebene Zeit muss kürzer sein als die für die Rufweiterschaltung konfigurierte Zeit (Standardeinstellung für die Rufweiterschaltung = 15 Sekunden). Siehe [Rufweiterschaltung konfigurieren](#).

- **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 Anrufübergabe prüfen:** Option

Bei aktivierter Option erfolgt eine Prüfung des Anwesenheitsstatus des Anrufziels. Bei einem anderen Anwesenheitsstatus als Büro wird der Anruf zum Kommunikationssystem zurückgestellt und das nächste CCV-Objekt verwendet.

- **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.

Tipp: 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 +49 eine deutsche Ansage und für eine Rufnummer mit der Ländervorwahl +33 eine französische Ansage abgespielt wird.

Eigenschaften:

- **Standardsprache:** 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 den zugehörigen (dem **Muster** entsprechenden) Rufnummern zugeordnet werden soll.

Eine Sprache kann beliebig vielen verschiedenen (dem **Muster** entsprechenden) Rufnummern 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 +49 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**). Es kann auch die Ortsvorwahl verwendet werden (z B. 089 für München).

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 Rufnummern, denen 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** +49 (=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 den zugehörigen (dem **Muster** entsprechenden) Rufnummern als Ziel zugeordnet werden soll.

Beliebig vielen verschiedenen (dem **Muster** entsprechenden) Rufnummern 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 Bedingungsangabe 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"

- **Datenverzweigung**

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 **LDAP-Daten1 (XMPP)** oder **LDAP-Daten2 (Pager)**.

Die Datenabfrage erfolgt über LDAP entweder direkt an eine LDAP-fähige Datenbank oder indirekt über den Directory Service (ODS) an eine SQL / ODBC-Datenbank. Die Abfrageergebnisse werden über die Zuordnung des LDAP-Feldes der UC Suite den entsprechenden Kriterien des Contact Centers zugewiesen. 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. Die Stichworte „Pager“ und „Info“ müssen unbedingt zugewiesen werden.

- **Zeitüberschreitung:** Zeitüberschreitung in Sekunden.
- **Verzweigung nach Zeitüberschreitung:** Aufklappliste zur Auswahl des CCV-Objekts, das bei einer Zeitüberschreitung als Ziel verwendet werden soll.
- **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.
- **Beschreibung:** Angabe einer Erläuterung.

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.

Dabei wird unterschieden zwischen:

- Einfache 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.

- Mehrfache 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. Hierzu kann entweder die Mehrfachauswahl oder die Funktion "**Alle auswählen**" verwendet werden. Darüber hinaus ist die Eingabe von Rufnummernmustern möglich. Rufnummernmuster setzen sich aus einer bestimmten Ziffernfolge und einer Wildcard (Platzhalter)

Multimedia Contact Center Rückfalllösung (Fallback-Lösung)

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. Die 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:

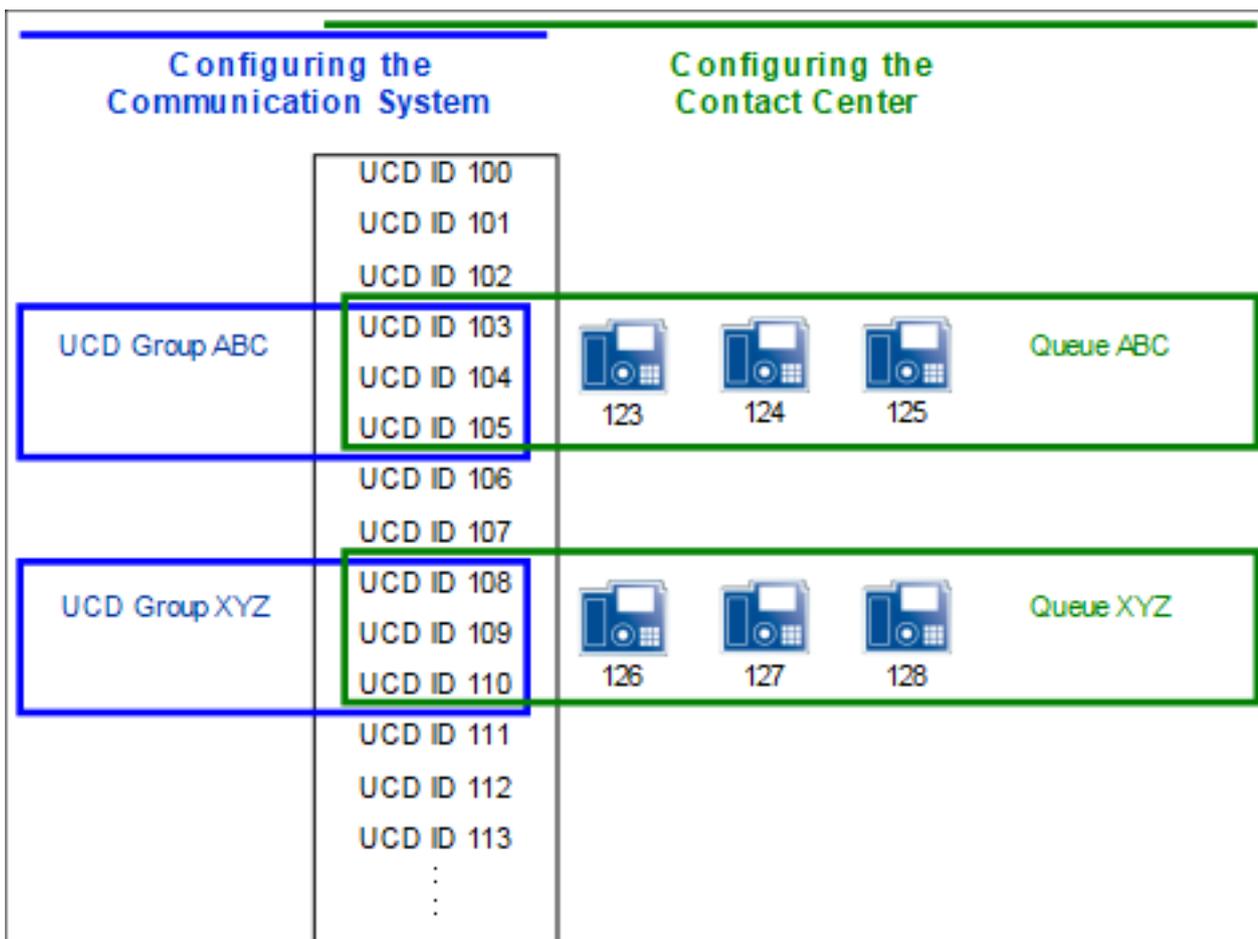
- Den UCD-Gruppen des Kommunikationssystems werden Agenten anhand von UCD-IDs zugeordnet. Die UCD-ID bestimmt, welcher UCD-Gruppe dieser Agent bei einem Ausfall des Contact Centers zugeordnet wird.

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 sind als Agenten mit den UCD-IDs 103, 104 und 105 konfiguriert. Die Teilnehmer 126, 127 und 128 sind 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

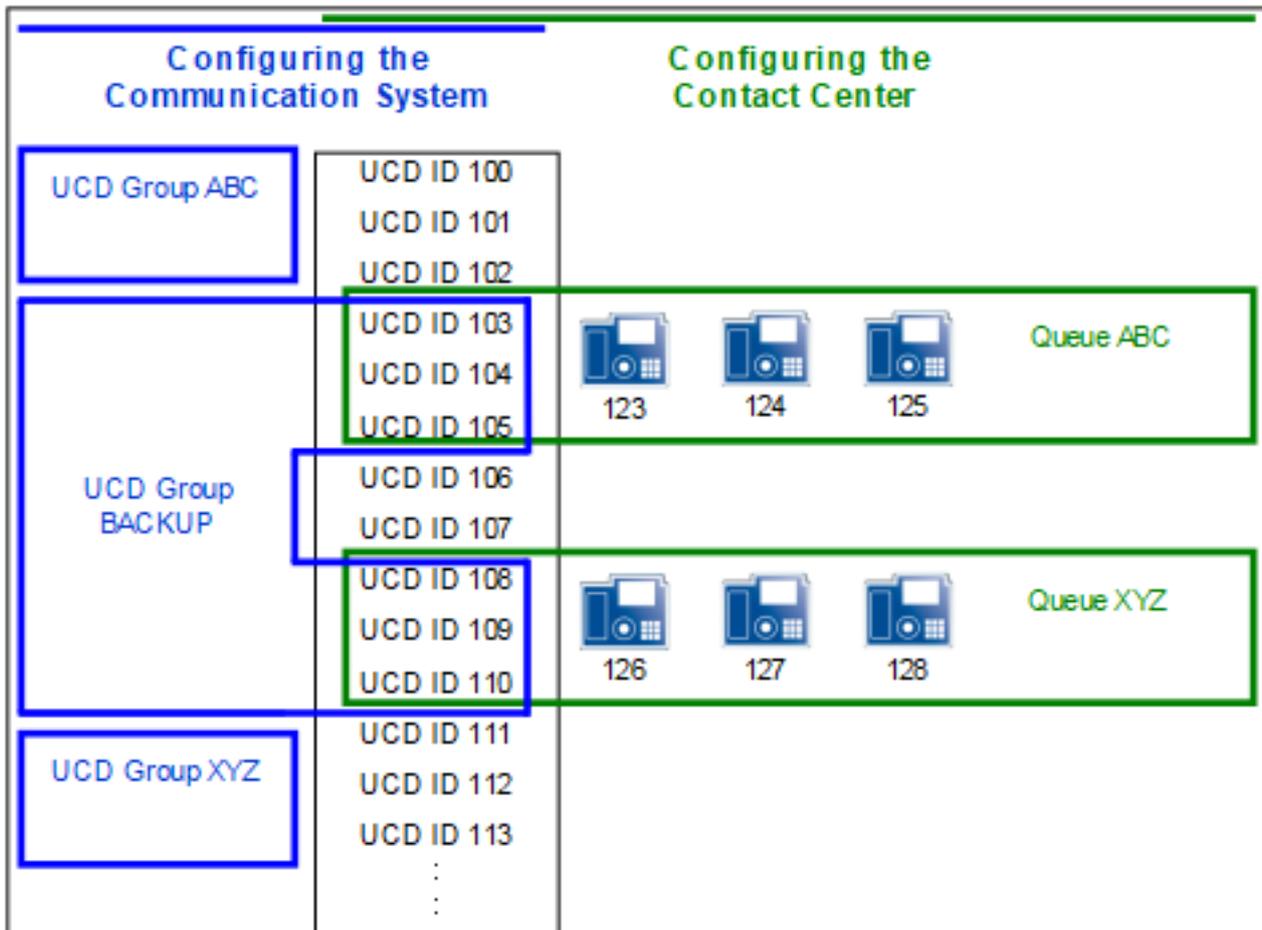
die Zuordnung der entsprechenden Agenten werden diese UCD-IDs dann auch in den Warteschlangen des Contact Centers verwendet. Damit ist gewährleistet, dass bei Ausfall des Contact Centers sich die Agenten nicht mit einer anderen ID manuell an ihrem Telefon neu anmelden müssen. Für alle UCD-Gruppen des Kommunikationssystems wird diese Backup-UCD-Gruppe als Rufweiterschaltungsziel definiert.

Anmerkung: Die konfigurierte Backup-UCD-Gruppe muss auch als Gruppe im Contact Center konfiguriert werden. Nur so ist sichergestellt, dass diese Gruppe ebenfalls überwacht wird.

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 sind als Agenten mit den UCD-IDs 103, 104 und 105 konfiguriert. Die Teilnehmer 126, 127 und 128 sind 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 [UCD \(Uniform Call Distribution\)](#) (Anrufverteilung).

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.

Tipp: 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.

Anmerkung: Das Abspielen von Ansagen ist nur über Amtsleitungen möglich. Um die Ansage abzuspielen, muss der Anruf von einer Amtsleitung kommen oder der Anrufer sollte von OpenScape Contact Center überwacht werden.

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 Rufweitschaltungsziel 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 Rufweitschaltungsziel 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
		Geschäftszeiten 13:00 Uhr bis 17:00 Uhr = Open2
Mittagspause	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 zuzuweisen.

Informationen über die Konfiguration aller Contact-Center-Funktionen finden Sie unter [Vorgehensweise bei der Konfiguration](#) .

17.6.2 Vorgehensweise bei der Konfiguration

Hier erhalten Sie einen Überblick über die bei der Konfiguration des Contact Centers durchzuführenden Tätigkeiten.

- 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.

- 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

Anmerkung: Das Abspielen von Ansagen ist nur über Amtsleitungen möglich. Um die Ansage abzuspielen, muss der Anruf von einer Amtsleitung kommen oder der Anrufer sollte von OpenScape Contact Center überwacht werden.

- 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

17.7 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_{PO/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, Regelasistenten 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/Rufnummerntausch**

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**

Multimedia Contact Center

Hinweise zum Einsatz von DECT-Telefonen

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

Tipp: 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 bis 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 Berichtsparemtern 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 einsetzbare 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.

Tipp: Berichte basieren auf der im Kommunikationssystem gespeicherten Anruflhistorie. Die maximale Aufbewahrungsdauer der Anruflhistorie beträgt 365 Tage (Standardeinstellung). Ein Administrator mit dem Profil **Expert** kann die Aufbewahrungsdauer der Anruflhistorie 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**

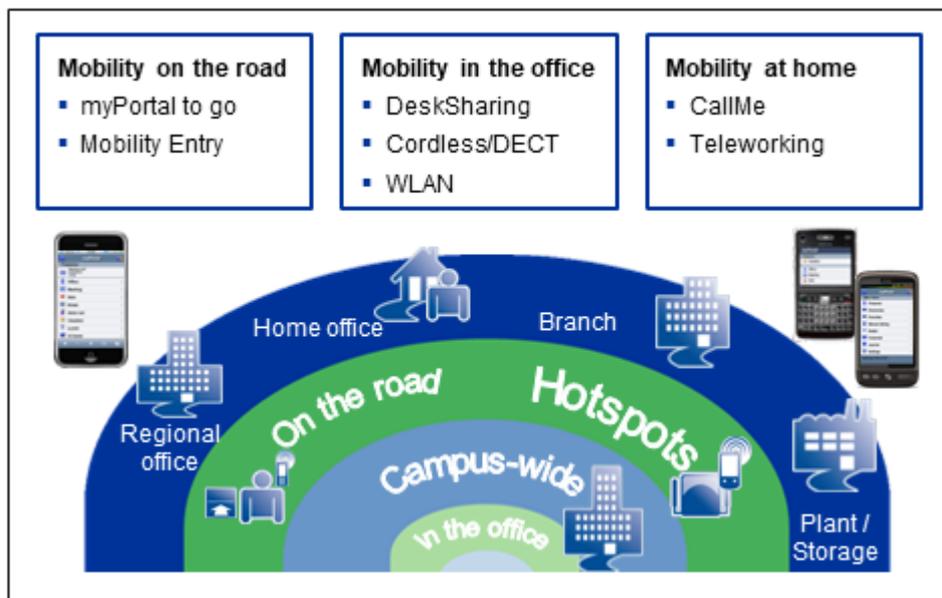
18 Mobility

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.

Zugehörige Konzepte
[Teilnehmer](#) auf Seite 209

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 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 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 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 5.0 oder höher)
- als Mobile UC App für das Betriebssystem Apple iOS (Version 12.5 oder höher)
- als Web Edition für mobile Web-Browser mit HTML5-Unterstützung, z. B. für die Betriebssysteme Windows Phone (Version 8.0 oder höher) oder Blackberry (Version 10 oder höher):

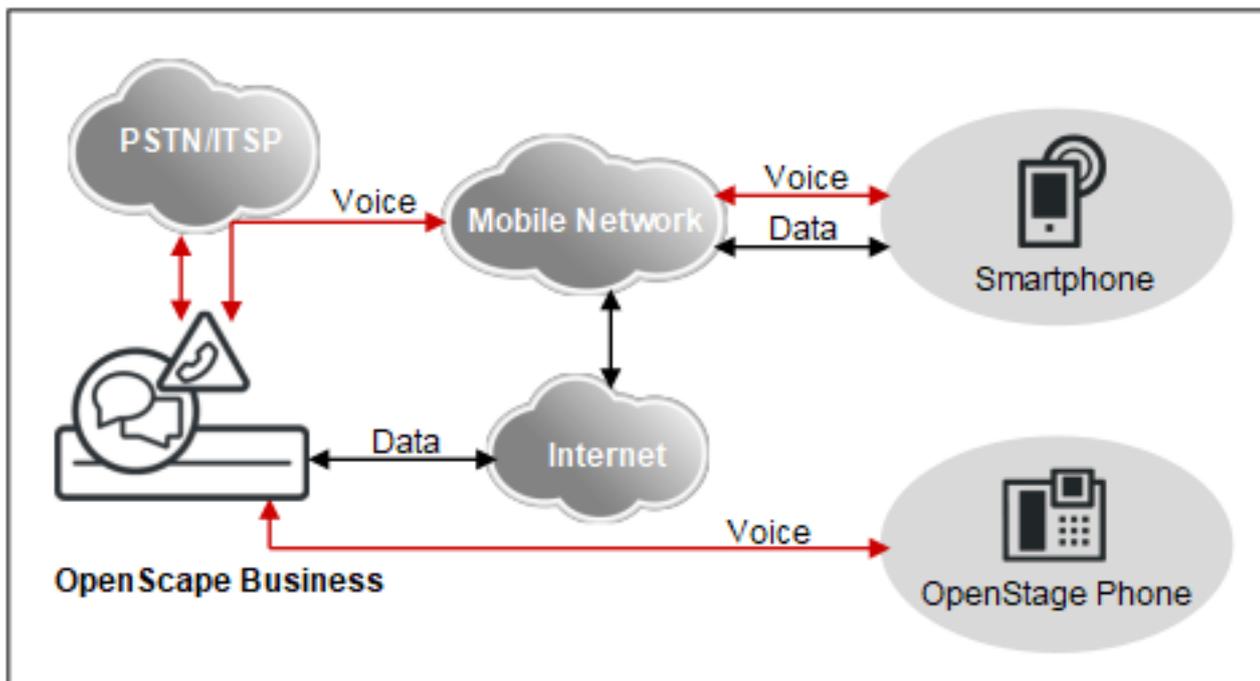
`http://<IP-Adresse des Kommunikationssystems>:8801`

`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.

Anmerkung: Bitte beachten Sie, dass bei Verwendung von myPortal to go Web Edition im Tischtelefon-Betriebsmodus keine Telefonie über den Client möglich ist. Sie können Anrufe tätigen, aber die Payload wird durch das verbundene Telefon geleitet.

myPortal to go kann sowohl auf reinen GSM-Mobiltelefonen als auch auf Dual-Mode-Telefonen genutzt werden. Für die Nutzung von myPortal to go ist ein Mobilfunkvertrag mit Datenoption (Flatrate empfohlen) erforderlich.



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 Namensuche
- Anruffunktionen
- One Number Service (ONS)
- Voicemail
- Textnachrichten

CTI-Leistungsmerkmale während eines Gesprächs:

- Rückfrage
- Makeln
- Attendant
- Konferenzschaltung
- Trennen

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 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.

Anmerkung: Zur Unterstützung der Mobilität muss myPortal to go zunächst als VoIP (HFA) Benutzer registriert werden, damit der für OpenScape Business System relevante Port aktiv wird.

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.

18.2.1.1 Voraussetzungen: myPortal to go

Um myPortal to go zu nutzen muss das Smartphone über geeignete Hardware und Software verfügen.

Es gelten folgende Anforderungen:

- myPortal to go als Mobile UC App: Android-Betriebssystem (Version 5.0 oder höher) oder Apple iOS (Version 12.5 oder höher)
- myPortal to go als Web Edition: Für mobile Web-Browser mit HTML5-Unterstützung, z.B. für Betriebssysteme Windows Phone (Version 8.1 oder höher) oder Blackberry (Version 10 oder höher). Webbrowser ohne TLS 1.2-Unterstützung werden nicht mehr unterstützt.

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.

- myPortal to go iOS-Client:
 - Es muss ein geeigneter DNS-Server konfiguriert und Internetzugang gewährt werden, damit öffentliche

Domännennamen aufgelöst werden können und Push-Benachrichtigungen über die APNS-Server von Apple an das iOS-Gerät gesendet werden können.

- Wenn die Firewall des Unternehmens den ausgehenden Internetzugang einschränkt, stellen Sie sicher, dass die Firewall für APNS auf Port TCP/443 offen ist.
- Für iOS-Push-Benachrichtigungen ist es zwingend erforderlich, die Systemsoftware auf dem neuesten Stand zu halten, da die obligatorischen Zertifikate für die Kommunikation mit dem APNS-Dienst von Apple häufig mit größeren/kleineren Systemversionen und Korrekturversionen aktualisiert werden.
- Die neuesten Versionen von myPortal to go (iOS) unterstützen die CallKit API von Apple. CallKit ist ein Framework, das darauf abzielt, das VoIP-Erlebnis zu verbessern, indem es myPortal to go (iOS) ermöglicht, sich in die nativen Anruhfunktionen des Geräts zu integrieren. Die erforderliche Mindestversion der Systemsoftware ist V3R2.

Aktuelle myPortal to go (iOS) Clients können sich nicht bei älteren OpenScape Business Versionen anmelden.

- Für die Verbindung zum Kommunikationsserver gelten die iOS-Sicherheitsanforderungen. Das aktuelle, von Openscape Business automatisch generierte, selbstsignierte Zertifikat ist nicht ausreichend, wenn die Anwendung eine Verbindung zum Kommunikationsserver über einen Domännennamen statt über eine Server-IP-Adresse herstellt. Apple hat seine Sicherheitsanforderungen für TLS-Serverzertifikate überarbeitet <https://support.apple.com/en-us/HT210176>.

Um Probleme zu vermeiden, wenn myPortal to go (iOS) keine Verbindung zum Kommunikationsserver herstellen kann, empfehlen wir, sich entweder über die IP-Adresse mit dem Kommunikationsserver zu verbinden oder ein vertrauenswürdige SSL-Zertifikat auf der Serverseite zu installieren.

- Touchscreen (empfohlen für komfortable Bedienung)
- Display-Auflösung für Smartphones: mindestens 240 Pixel * 320 Pixel (empfohlen: 320 Pixel * 480 Pixel oder höher)
- Display-Auflösung für Tablet-PCs: mindestens 800 Pixel * 480 Pixel (empfohlen: 1024 Pixel * 600 Pixel oder höher)
- Internet-Zugang
- 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.

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.

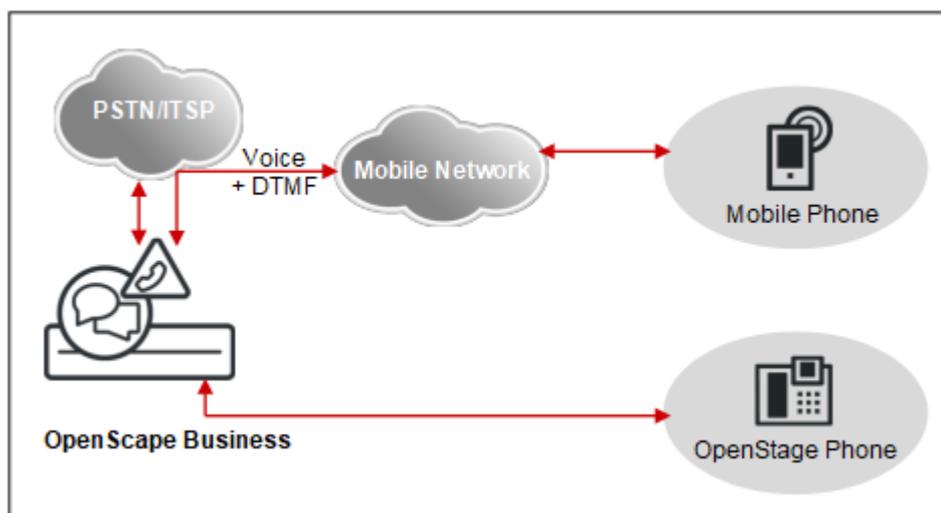
Die Mobile UC App kann kostenfrei im Google Play Store oder im Apple App Store heruntergeladen werden.

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 Freigabemitteilung und im Experten-Wiki unter https://wiki.unify.com/wiki/myPortal_to_go.

18.2.2 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:

- Rückruf
- 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
- Anrufschatz 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).

Anmerkung: 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.

Anmerkung: Mobility Entry darf nur an Knoten mit direktem Amtszugang konfiguriert werden.

Zugehörige Konzepte

[One Number Service](#) auf Seite 540

[Vergleich Mobile Clients und Mobility Entry](#) auf Seite 537

[Abhängigkeiten für Mobile Clients und Mobility Entry](#) auf Seite 538

18.2.3 Vergleich Mobile Clients und Mobility Entry

Die Mobile Clients myPortal for Mobile und myPortal to go und Mobility Entry unterstützen unterschiedliche Leistungsmerkmale.

Leistungsmerkmal	myPortal to go	Mobility Entry
Allgemeine Funktionen		
Mobilfunkvertrag mit Datenoption	Ja (Flatrate empfohlen)	Nein
Parallele Rufsignalisierung an Systemtelefon und Mobiltelefon (Twinning)	Ja	Ja
Übertragung der Anrufer-Rufnummer zum Mobiltelefon (wenn das Netz externe Rufnummern als CLIP überträgt, CLIP no Screening)	Ja	Ja
One Number Service (wenn das Netz externe Rufnummern als CLIP überträgt, CLIP no Screening)	Ja	Ja
Anrufschutz/abschaltbare Anrufweiterleitung	Nein	Ja
Rufnummernunterdrückung ein-/ausschaltbar	Nein	Ja
Automatische Identifizierung registrierter Teilnehmer	Ja	Ja
Betrieb ohne Bürotelefon (als virtueller Teilnehmer)	Ja	Ja
Nutzbar mit OpenScape Business S	Ja	Ja
Anwesenheitsstatus, Journal, Sprachbox		
Eigenen Anwesenheitsstatus ändern	Ja	Nein
Anwesenheitsstatus anderer Teilnehmer sehen	Ja	Nein
Journal	Neue, Alle, Entgangen, Angenommen, Ankommend, Sprachnachrichten	Nein
Gemeinsame Sprachbox, Abfrage auch von unterwegs möglich	Ja	Ja
Anzeige eingegangener Sprachnachrichten	Anzeige neuer, abgehörter und gespeicherter Sprachnachrichten	Nein
Wählen		
Zugriff auf Kontakte im Mobiltelefon	Ja	Ja

Mobility

Leistungsmerkmal	myPortal to go	Mobility Entry
Zugriff auf Kontakte im Kommunikationssystem	Externes Verzeichnis (UC Suite), internes Verzeichnis, persönliche Kontakte und Systemtelefonbuch	Nein
Favoriten	Ja	Nein
Manuelle Wahl	Ja	Ja
Wahlwiederholung	Ja	Nein
Wahlverfahren	Callback, Call Through, Assoziierte Wahl	Callback, Call Through
Während des Gesprächs		
Rückfrage	Ja (nicht mit SIP-Telefon)	Ja
Makeln	Ja (nicht mit SIP-Telefon)	Ja
Vermitteln	Ja (nicht mit SIP-Telefon)	Ja
Konferenz	Ja (nicht mit SIP-Telefon)	Ja
Rückruf bei Frei und Besetzt	Nein	Ja
Anrufübernahme vom Mobiltelefon auf das Systemtelefon	Ja	Ja
Besetztanzeige auch bei Gesprächen am Mobiltelefon (bei One Number Service)	Ja	Ja

Zugehörige Konzepte

[Mobility Entry](#) auf Seite 535

18.2.4 Abhängigkeiten für Mobile Clients und Mobility Entry

myPortal to go und Mobility Entry besitzen Abhängigkeiten zu anderen Leistungsmerkmalen (z.B. zu DISA).

Abhängigkeit	myPortal to go	Mobility Entry
Mobility-Callback-DuWa	Beim Wahlmodus Mobile Callback muss die Mobility-Callback-Durchwahlnummer konfiguriert sein.	

Abhängigkeit	myPortal to go	Mobility Entry
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.	
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.	-
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.	-

Abhängigkeit	myPortal to go	Mobility Entry
Datenverbindung	Es wird empfohlen einen Mobilfunkvertrag mit Datenflatrate abzuschließen. Nutzer von Volumentarifen sollten in den Einstellungen von myPortal to go die Option "Automatisches Refresh" ausschalten.	-
Parallele Verbindungen	Für einige Leistungsmerkmale ist eine gleichzeitige Sprach- 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, die DTMF-Übertragung unterstützen.

Zugehörige Konzepte

[Mobility Entry](#) auf Seite 535

18.2.5 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.

Zugehörige Konzepte

[Mobility Entry](#) auf Seite 535

18.2.6 Dual-Mode-Telefonie

Dual-Mode-Mobiltelefone unterstützen sowohl GSM/UMTS-Netze als auch WLAN-Netze. SIP-Teilnehmer oder System-Clients (d.h. HFA-Teilnehmer) können sich über WLAN am Kommunikationssystem registrieren.

Befindet sich das Dual-Mode-Mobiltelefon in WLAN-Reichweite, wird es automatisch als SIP-Teilnehmer oder System-Client (HFA-

Teilnehmer) gerufen. Außerhalb der WLAN-Reichweite wird das Dual-Mode-Mobiltelefon über GSM/UMTS gerufen (Mobiltelefon-Integrations-Leistungsumfang möglich).

Anmerkung: Der Dualmodus für HFA wird nur bei Verwendung des myPortal to Go-Clients und nicht bei anderen Geräten oder Clients unterstützt.

Das automatische Weiterleiten an die GSM-Rufnummer funktioniert nur dann, wenn der zugehörige HFA- oder SIP-Teilnehmer im System als Mobiltelefon-Teilnehmer eingetragen ist (Mobiltelefon Integration). Das bedeutet, wenn der HFA- oder SIP-Teilnehmer registriert ist, wird er als HFA- oder SIP-Teilnehmer gerufen, wenn nicht, dann wird er über die in der Mobiltelefon-Integrations-Konfiguration zugeordnete GSM-Rufnummer gerufen. CTI-Anruffunktionen sind für SIP-Clients nicht in myPortal to go verfügbar. Stattdessen erfolgt die Steuerung gegebenenfalls innerhalb des HFA- oder SIP-Clients (siehe auch Freigabemittteilung 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.

18.2.7 Konfiguration von myPortal to go und Mobility Entry

myPortal to go (Web Edition) und Mobility Entry werden mit dem Wizard **Mobiltelefon Integration** konfiguriert.

Mit dem Wizard **Mobiltelefon Integration** kann der Administrator:

- One Number Service einrichten
- myPortal to go (Web Edition) 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, wird 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 to go (Web Edition) 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.

Zugehörige Konzepte

[Konfiguration von Teamschaltungen / Team-Gruppen und Chef/Sekretär-Funktionen / Top-Gruppen über Wizards](#) auf Seite 390
[Voraussetzungen für Application Launcher](#) auf Seite 681

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)
- Konferenzschaltung
- Aufschalten
- Makeln
- Parken
- Rückfrage
- Übergeben
- Anrufübernahme
- Anrufschutz
- Anrufumleitung
- Info senden (Message Waiting)
- Rückruf
- Rufnummernunterdrückung
- Rufzuschaltung

Anmerkung: 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 sein. Außerdem muss Relocate/Rufnummerntausch 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/der 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.

Anmerkung: Das DeskSharing-Feature muss mit IP Station Port 3 oder höher verwendet werden.

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 (DECT Light)
- Für OpenScape Business X8: Anschaltung an die $U_{P0/E}$ -Schnittstellen einer SLMUC- (SLMU und CMAe)

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 > Telefonie > Cordless > Systemweit**). Eine Konfiguration an den DECT-Telefonen ist nicht notwendig. Ein manueller Restart des Systems ist erforderlich, um das Leistungsmerkmal bei OpenScape Business X1, X3, X5 zu aktivieren

- 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 [Konfiguration der integrierten Cordless-Lösung](#).

Baugruppen und Basisstationen

Die Beschreibung der Baugruppen und Basisstationen finden Sie unter *OpenScape Business Servicedokumentation in den Kapiteln Baugruppen und Basisstationen*.

18.3.2.1 Systemübersicht

Die Anschaltung der OpenScape Business Basisstationen erfolgt bei OpenScape Business X3/X5 entweder direkt an den $U_{P0/E}$ -Schnittstellen des Mainboards oder an den $U_{P0/E}$ -Schnittstellen einer installierten SLU8N/SLU8NR-Baugruppe (DECT Light). Bei OpenScape Business X8 können die Basisstationen an den Cordless-Baugruppen SLMUC angeschlossen werden.

Direktanschaltung (DECT Light)

Die Basisstationen können direkt an den $U_{P0/E}$ -Schnittstellen von OCCM, OCCMB, OCCMA und OCCMR, OCCMBR, OCCMAR der Kommunikationssysteme OpenScape Business X3R/X3W und OpenScape Business X5R/X5W angeschlossen werden oder an den $U_{P0/E}$ -Schnittstellen einer SLU8N/SLU8NR-Baugruppe.

Durch Einsatz des Submoduls CMAe auf den Mainboards werden die Funktionen ADPCM-Wandlung und Echokompensation zur Verfügung gestellt (48 Kanäle für CMAe). Es können bis zu vier Gespräche pro Basisstation geführt werden. Bis zu sieben Basisstationen können an die $U_{P0/E}$ -Schnittstellen der Mainboards OCCM, OCCMB, OCCMA und OCCMR, OCCMBR, OCCMAR angeschlossen werden.

Falls kein CMAe installiert ist, können maximal zwei Gespräche pro Basisstation geführt werden. In diesem Fall wird die ADPCM-Wandlung direkt von der DECT-Basisstation durchgeführt.

Anmerkung: Wenn kein CMAe installiert ist, stehen keine Echo Handling-Funktionen zur Verfügung.

Für die Anschaltung von Basisstationen an eine SLU8N/SLU8NR-Baugruppe 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 ist 64 bei einem CMAe.
- 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 Ports 2 und 3 der Basisstation werden 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.

Cordless-Baugruppenanschaltung

Die Basisstation BS5 kann an die $U_{P0/E}$ -Schnittstellen der folgenden Cordless-Baugruppen angeschlossen werden:

- SLMUC (SLMU + CMAe bei OpenScape Business X8 (siehe Kapitel zu *SLMUC-Servicedokumentation*))

Der Anschluss der Basisstationen kann über eine, zwei oder drei $U_{P0/E}$ -Schnittstellen erfolgen. Die letzten 8 Schnittstellen können nur als zweite oder dritte U_{P0} -Schnittstellen der Basisstation verwendet werden. Der zusätzliche Anschluss von $U_{P0/E}$ -Schnittstellen erhöht Verkehrswert der angeschlossenen Basisstation und damit die Anzahl der gleichzeitig verfügbare Gesprächskanäle.

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.

Wenn keine SLCN- oder SLC16N-Baugruppen vorhanden sind und die BS über $U_{P0/E}$ verbunden ist, wird auf der Steuerungsbaugruppe ein CMA- oder CMAe-Modul benötigt, wenn im OpenScape Business-Netzwerk CMI-Roaming vorgesehen ist.

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.

Anmerkung: Die Basisstationen BS4 (S30807-U5491-X), 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.

Tipp: Falls kein CMA/CMAe installiert ist, können maximal zwei Gespräche pro Basisstation geführt werden. In diesem Fall wird die ADPCM-Wandlung direkt von der DECT-Basisstation durchgeführt. Die Echokompensation wird jedoch nicht direkt unterstützt. Falls Echokompensation erforderlich ist, wird ein CMA/CMAe-Submodul benötigt.

Anmerkung: In der folgenden Tabelle wird die Kombination aus SLMU-Karte und CMAe-Modul als SLMUC bezeichnet.

OpenScape Business	Maximale Anzahl Baugruppen				Clock Module	Max. Anzahl der Basisstationen bei Anschluss über 1xU _{P0}	Ports / gleichzeitige Gespräche pro BS	Max. Anzahl der registrierter Geräte	Max. Anzahl gleichzeitiger Rufe
	SLC16N	SLCN	SLUN	SLMUC					
X1	-	-	-	-	-	7	1/2	16	14
	-	-	-	-	CMA	7	1/4	16	16
	-	-	-	-	CMAe	7	1/4	16	16
X3	-	-	-	-	-	7	1/2	32	16
Onboard U _{P0/E} (SLUC)	-	-	-	-	CMA	7	1/4	32	16
	-	-	1	-	CMA	15	1/4	32	16
	-	-	-	-	CMAe	7	1/4	64	28
	-	-	1	-	CMAe	15	1/4	64	48
X5	-	-	-	-	-	7	1/2	32	16
	-	-	-	-	CMA	7	1/4	32	16
	-	-	1	-	CMA	15	1/4	32	16
	-	-	-	-	CMAe	7	1/4	64	28
	-	-	1	-	CMAe	15	1/4	64	48
X5W	1	-	-	-	-	16	3/12	64	32*

OpenScape Business	Maximale Anzahl Baugruppen				Clock Module	Max. Anzahl der Basisstationen BS bei Anschluss über 1xUp0	Ports / gleichzeitige Gespräche pro BS	Max. Anzahl der registrierter Geräte	Max. Anzahl gleichzeitiger Rufe
	SLC16N	SLCN	SLUN	SLMUC					
X8	-	4	-	-	-	64	3/12	250 (128 pro SLCN)	128**
	-	-	-	4	CMAe	64	3/12	250 (128 pro SLCN)	192***

* Maximalwert je SLCN16 ist 32. Beim Roaming erfolgt die ADPCM-Wandlung immer auf der SLC16N-Baugruppe, an der sich gerade das Mobilteil befindet. Daher könnte die Anzahl gleichzeitiger Anrufe pro System höher als 32 sein, wenn sich das Mobilteil an der Gast-SLC16N befindet

** Der Maximalwert je SLCN ist 32. Je nach Standort der Mobilteile beim Roaming könnten theoretisch alle registrierten Geräte (250) aktiv sein, wenn 4 SLCN-Karten verfügbar sind.

*** SLCN und SLMUC können in einem System kombiniert werden. Der Maximalwert ist 32 je SLCN und 48 je SLMUC. Je nach Standort der Mobilteile beim Roaming könnten theoretisch alle registrierten Geräte (250) aktiv sein, wenn insgesamt 4 SLCN/SLMUC verfügbar sind.

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 ausgetauscht, 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 wird das Mobilteil automatisch abgemeldet. Und zur Sicherheit ist es nicht mehr möglich, in Kenntnis der alten PIN, ein Mobilteil missbräuchlich anzumelden.

18.3.2.5 Bedeutung der Ergebnisse beim Test des Funkbereichs

Wichtig:

Ergebnisse, die von einem Mobiltelefon erhoben wurden, sind nicht sehr genau und dienen nur einer groben Einschätzung. Von jedem Mobiltelefon werden zudem, unter sonst gleichen Bedingungen,

unterschiedliche Werte gemessen. Wenn Sie genauere Ergebnisse brauchen, empfehlen wir die Verwendung des Hicom Cordless Service Tool (HCS-DECT).

Die folgende Abbildung zeigt eine Beispielanzeige der Messergebnisse bei einem Gigaset Mobiltelefon während eines Anrufs:

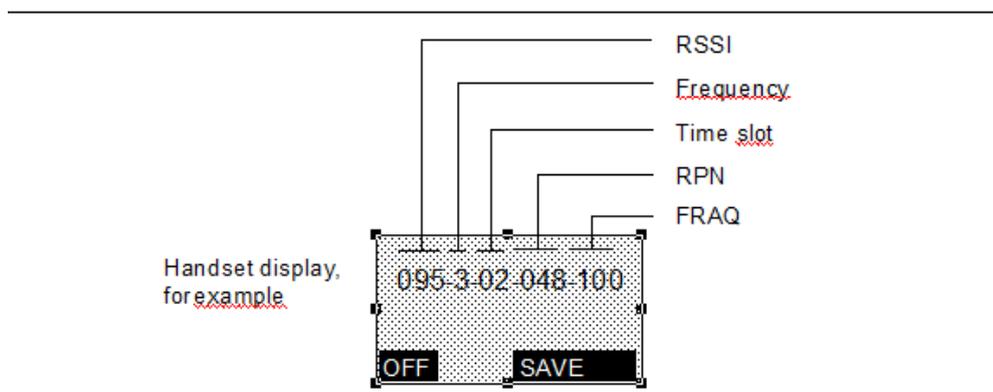


Abbildung 6: Messergebnis

Kapitel	Beschreibung
RSSI (Funksignal)	Feldstärke, der von der Basisstation empfangenen Funksignale, normiert auf maximal 100. Bei einem Wert <50 ist die Funkverbindung zur Basisstation nicht mehr sichergestellt. Eine akzeptable Feldstärke liegt bei >50 (> - 60 dBm).
Frequenz	Frequenz (0 - 9)
Zeitschlitz (Slot)	Zeitschlitz (0 - 11) des Empfangskanals, auf dem die Messung durchgeführt wurde.

Kapitel	Beschreibung
RPN (Portnummer)	<p>OpenScape Business X1/X3/X5/X8</p> <p>ID der Basisstation, zum Beispiel, 048, Portnummer in den SLC-Baugruppen. Wenn das Mobilteil in eine überschneidende Funkzelle/ Basisstation wechselt, wird die aktuelle Portnummer (wo der D-Kanal der Basisstation konfiguriert ist) auf dem Display angezeigt. Formel: $A \times 16 + B$ A = Nummer der SLC-Baugruppe (1 - 127); 16 = Faktor B = Port der zugewiesenen SLC-Baugruppe (wo der D-Kanal der Basisstation konfiguriert ist) Beispiele: RPN = 1 x 16 + Port 0 = 016 RPN = 2 x 16 + Port 8 = 040.</p> <p>Die Portnummer (PRN) wird für die Geräte Gigaset S3 Professional und Gigaset SL3 Professional in hexadezimaler Form mit angehängtem H angezeigt. Der hexadezimale Wert wird ohne angehängtes H angezeigt, z.B. "-028-" bei den Geräten Gigaset S4 Professional und OpenStage SL4 Professional. Beispiel: Wenn zuvor der Wert 040 angezeigt wurde, wird jetzt für das Gigaset S3/SL3 Professional der Wert 028H angezeigt. Die hexadezimale Darstellung unterscheidet sich nur durch angehängtes oder nicht angehängtes „H“. Dies gilt auch für OpenScape DECT Phone S5/SL5/S6/SL6/R6 Geräte (kein vorangestelltes H vorhanden).</p>
FRAQ (Frame Quality)	<p>Übertragungsqualität in %. 95 % bis 100 % zufriedenstellend (für kurze Zeiträume 90% bis 94 % nicht kritisch), < 95 % fehlerhaft.</p>

Weitere Informationen zum Menü der Messung, siehe:
*OpenScape Cordless Enterprise, Servicedokumentation, Kapitel:
 Testen des Funkbereichs und OpenScape Business X3/X5/X8,
 Servicedokumentation, Kapitel: Funkabdeckung prüfen.*

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 CMAe-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)

18.3.4 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 folgende Arten von Teleworking-Teilnehmern:

- VPN-Teilnehmer

OpenScape Business verfügt über eine integrierte 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).

- Gerät@Home: SIP@Home-Teilnehmer oder Systemgerät@Home-Teilnehmer

STUN-fähige SIP-Telefone (z.B. Yealink T19) (SIP-Gerät@Home-Teilnehmer) oder HFA-Telefone (Systemgerät@Home-Teilnehmer) 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 oder HFA-Telefon aktiviert werden.

Im WBM muss zusätzlich ein STUN-Server angegeben werden, wenn kein ITSP verwendet wird oder der genutzte ITSP keinen STUN-Server anbietet.

SIP-Gerät @Home unterstützt nicht die Übertragung von Video-Signalen.

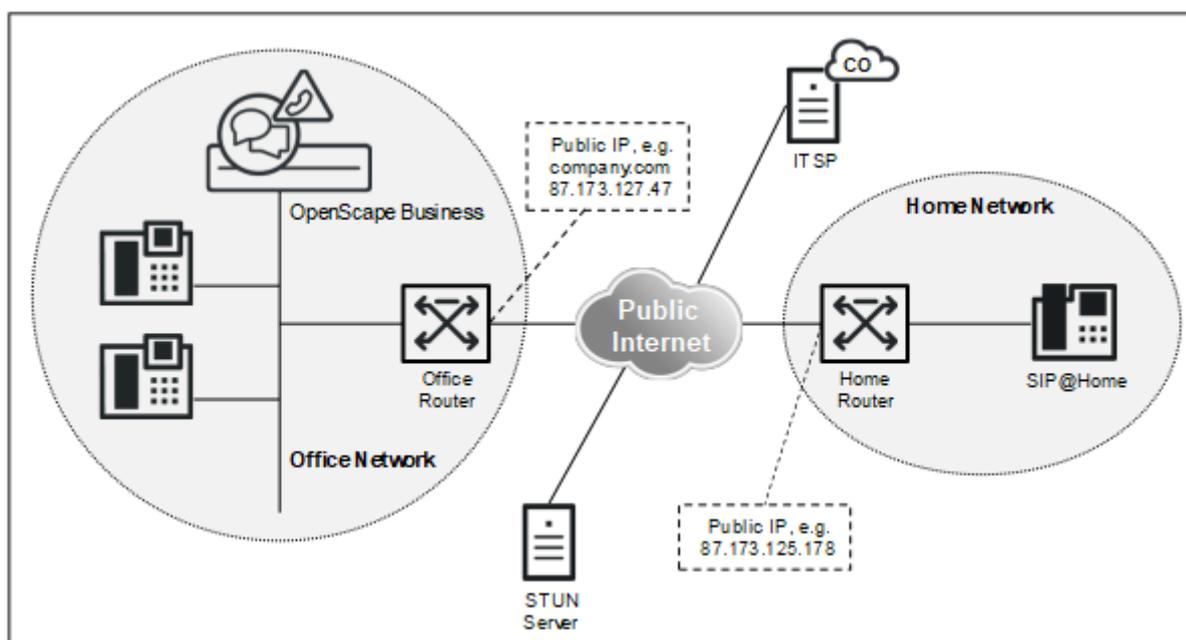


Abbildung 7: Gerät@Home (SIP-Gerät@Home- oder Systemgerät@Home-)Komponenten

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-Gerät@Home

Um Verbindungen über das Internet von einem STUN-fähigen SIP-Telefon zu OpenScape Business über das Internet herzustellen, sind bestimmte Konfigurationen durchzuführen.

Konfiguration von 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 Gerät@Home aktivieren](#)).

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 ein STUN-Server im System konfiguriert werden (siehe [Wie Sie einen STUN-Server für Gerät@Home angeben](#)).

Konfiguration des Office-Internet-Routers

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 9: Portweiterleitung im Office-Router konfigurieren

Transport	Interner SIP-Port	Externer SIP-Port	Kommentar
UDP	5070	Eingabe von z. B. 5090.	Für die Portweiterleitung müssen externer und interner SIP-Port nicht gleich sein. Als externer SIP-Port kann somit ein vom internen Standard-SIP-Port 5070 abweichender Wert eingegeben werden. Daher wird UDP empfohlen.
TCP	5070 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 5070 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.
TLS	5071	Eingabe von 5071 (= interner SIP-TLS-Port)	Für die Portweiterleitung müssen externer und interner SIP-TLS-Port gleich sein. Da bereits der interne SIP-TLS-Port vom Standard-SIP-TLS-Port abweicht, kann als externer SIP-TLS-Port auch 5071 eingegeben werden. Daher wird TLS empfohlen.

Anmerkung: In einem aktualisierten System wird eine Änderung der SIP-Ports nicht automatisch durchgeführt. Nach der Aktualisierung sind die Ports:

SIP_EXT = 5060

SIP_TLS_SUB_EXT = 5062

Diese Werte müssen vom Administrator manuell vorgenommen werden, wenn Gerät@Home im migrierten System genutzt wird.

Für TLS müssen im Kommunikationssystem gültige Zertifikate aktiviert sein. TLS Verbindungen für SIP-Teilnehmer werden an der

LAN-Schnittstelle des Kommunikationssystems unterstützt, nicht aber an der WAN-Schnittstelle. SRTP-Payload mit SDES-Signalisierung wird nicht unterstützt.

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 Störungen führen.

Konfiguration SIP-Telefon

Als Konfigurationsbeispiel finden Sie eine Liste aller getesteten SIP-Telefone, die STUN unterstützen, im Internet im Unify Experts Wiki. Sie finden dort die Werte, die am SIP-Telefon eingegeben werden müssen.

Konfiguration des Home-Internet-Routers

Am Home-Internet-Router ist keine spezielle Konfiguration erforderlich.

Folgende Anforderungen muss der Home-Internet-Router erfüllen:

- Der Router muss VoIP-Funktionalität mit eingeschalteter NAT zur Verfügung stellen (keine symmetrische NAT).
- Die ALG-Funktion muss im Router deaktiviert sein.

Die Internetverbindung muss genügend Bandbreite für die Gesprächsübertragung zur Verfügung stellen. Besonders bei asymmetrischen DSL-Verbindungen ist auf genügend Upload-Bandbreite zu achten.

myPortal @work konfigurieren

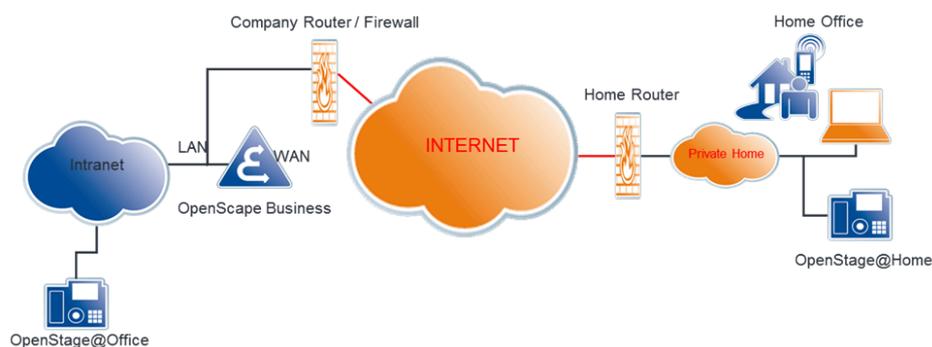
Damit myPortal @work über das Internet auf das Kommunikationssystem zugreifen kann, müssen Sie Folgendes durchführen:

- STUN-Server für System/Client konfigurieren
- Port 8802 öffnen und weiterleiten (andere Weiterleitungen sind ungültig)
- Das SBC-Flag wird nicht benötigt. Es ist keine Authentifizierung erforderlich.

18.4.3 Konfiguration für Systemgerät@Home

Um Verbindungen über das Internet von einem Systemgerät-Telefon zur OpenScape Business herzustellen, sind bestimmte Konfigurationen an OpenScape Business, dem Office-Internet-Router und dem Systemgerät-Telefon durchzuführen.

- **Abbildung 8: Beispiel für einen Systemgerät@Home-Anwendungsfall**



Konfiguration von OpenScape Business

Damit sich ein Systemgerät@Home-Teilnehmer über das Internet am Kommunikationssystem registrieren kann, muss für den Systemgerät@Home-Teilnehmer die integrierte SBC-Funktion aktiviert werden (siehe [Wie Sie Gerät@Home aktivieren](#)).

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 Kommunikationssystem ein STUN-Server bekanntgegeben werden (siehe STUN-Server für Systemgerät@Home angeben).

Konfiguration des Office-Internet-Routers

Damit Systemgerät@Home-Teilnehmer das Kommunikationssystem über das Internet erreichen können, muss im Office-Internet-Router eine Portweiterleitung für den Systemgerät-Port eingerichtet werden. Um sich aus dem Internet registrieren zu können, muss im Office-Router bzw. in der Firewall eine Regel für Portweiterleitung eingerichtet werden:

- externer Port TCP/4060 zu interner Port TCP/4062 (HFA), für nicht-TLS
- externer Port TCP/4061 zu interner Port TCP/4063 (HFA), für TLS

Anmerkung: Während der Migration von V2R1 auf eine höhere Version sollte der Office-Internet-Router entsprechend dieser Regel umkonfiguriert werden.

Die oben genannten Ports werden nur für Systemgeräte (HFA-Telefon) benötigt.

- RTP-Port-Bereich für OpenScape Business X: 30274-30529.
RTP-Port-Bereich für OpenScape Business S: 30528-30887 (Standardwerte)
- VoIP-fähige UC-Clients wie myPortal to go, myPortal @work benötigen diese Ports ebenfalls.
- TCP/8802 (HTTPS) (erforderlich für den Unified Communications-Client (z. B. myPortal to go, my Portal to go Web, my Portal @work

oder VoIP für myPortal to go, wenn als Systemgerät@Home konfiguriert)

Anmerkung: Die interne Firewall-Zone muss geschlossen werden.

Das Transport-Protokoll ist am Systemgerät@Home-Teilnehmer einzustellen.

Ist der Office-Internet-Router ohne feste IP-Adresse mit dem Internet verbunden, muss im Office-Internet-Router DynDNS konfiguriert sein, damit der Systemgerät@Home-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 Störungen führen.

Konfiguration des Home-Internet-Routers

Am Home-Internet-Router ist keine spezielle Konfiguration erforderlich.

Folgende Anforderungen muss der Home-Internet-Router erfüllen:

- Der Router muss VoIP-Funktionalität mit eingeschalteter NAT zur Verfügung stellen (keine symmetrische NAT).
- Die ALG-Funktion muss im Router deaktiviert sein.

Die Internetverbindung muss genügend Bandbreite für die Gesprächsübertragung zur Verfügung stellen. Besonders bei asymmetrischen DSL-Verbindungen ist auf genügend Upload-Bandbreite zu achten.

Konfiguration des HFA-Telefons

Das Gateway muss mit dem DNS-Namen (z.B. meinefirma.net) so konfiguriert werden, dass das Telefon das System über das Internet erreichen kann. Die IP von DLI muss auch konfiguriert werden. Für den Teilnehmer muss eine interne Rufnummer hinzugefügt werden. Außerdem muss das Gerätepasswort festgelegt werden.

Einschränkungen

- Die Konfiguration von XML-Anwendungen an OpenStage ist nicht möglich.

19 Sicherheit

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.

Portnummern

Anmerkung: 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 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 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 standardmäßig 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.

Anmerkung: 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.

19.1.1.2 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.

19.1.2 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.

19.1.3 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)

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.

Anmerkung: 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.

19.1.4 Dienstverwaltung (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.

Anmerkung: 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.

19.2 Signaling- und 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 Schlüsseln bereitstellen.

Die Schlüssel bzw. Zertifikate werden durch den DLS-Server verteilt (können aber auch manuell verteilt werden).

Tipp: Die SPE-Funktion wird nicht für SIP- und WL2-Teilnehmer angeboten.

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						
	Column1	HFA Subscriber	SIP Subscriber	TDM Subscriber	Analog Subscriber	SIP-Q Trunking	ISDN CO	FAX (T38, G711)	Column2	HFA Subscriber2	SIP Subscriber2	TDM Subscriber2	Analog Subscriber2	IP-Q Trunking (G W)
OpenScope 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:

Signaling Encryption	
nv	Keine VoIP Sicherheit

t	Standard: TLS auf der VoIP Seite; keine End-to-end Secure Payload
s	Signaling- und Payload-Encryption (SPE)
*	Keine End-to-end Signaling Encryption (TLS)
Payload Encryption	
y	Secure Payload (SRTP)
n	Non-Secure Payload (RTP)

19.3 Virtual Private Network VPN

Ein VPN (Virtual Private Network) ist ein PC-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.

Übersicht VPN

VPN bietet Ihnen:

- Sichere Verbindung über ein ungeschütztes Medium (Internet)
- Schutz vertraulicher Daten vor Manipulation
- Sichere Integration von externen Partnern ins Firmennetz
- Zugriff auf Unternehmensinformationen für den Außendienst

Um eine sichere Kommunikation zu gewährleisten, funktioniert VPN folgendermaßen: Es wird ein Tunnel zwischen den Kommunikationspartnern aufgebaut. Bei diesem Tunnelaufbau findet eine Authentifizierung und Autorisierung statt. Nach dem Tunnelaufbau werden die eigentlichen Daten verschlüsselt übertragen.

Ein VPN kann zwischen (mindestens) zwei Rechnern 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 für die VPN-Parameter erfolgt prinzipiell 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

Themenbereich	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:

Länge des ESP-Headers

Padding

Bandbreiten-Kalkulation für den Verschlüsselungs-Algorithmus AES:

Bandbreiten-Kalkulation für den Verschlüsselungs-Algorithmus DES / 3DES:

Bandbreite für Fax T.38

Protokoll	Bytes	
ESP Trailer	12	
ESP Padding	variiert (y)	Verschlüsselt
ESP Padding Header	2	Verschlüsselt
Sprach-Payload	variiert (x)	Verschlüsselt

Protokoll	Bytes	
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	

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 ist erforderlich, da die Verschlüsselungs-Algorithmen auf Blockchiffrierung 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:

$$(42 + x + y) \text{ (Bytes)} = N \times (0 \text{ oder } 16 \text{ (Bytes)}) \text{ (N integer)}$$

Codec	Paketierun-Parameter	Rahmengr (ms)	Payload (Bytes)	Padding (Bytes)	Ethernet Paketlänge (Bytes)	Payload/ Packet overhead ration	Ethernet Load (inkl. Header) (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

Sicherheit

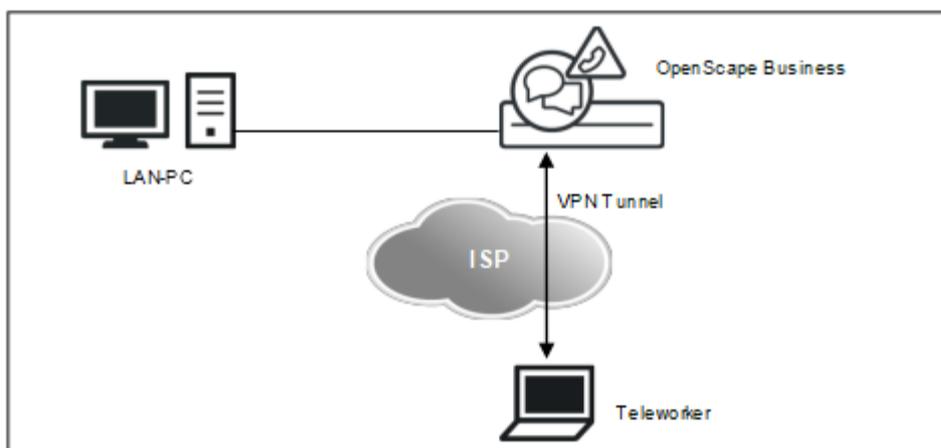
Codec	Paketierungsparameter	Rahmengröße (ms)	Payload (Bytes)	Padding (Bytes)	Ethernet Paketlänge (Bytes)	Payload/ Packet overhead ration	EthernetLoad (inkl. Header) (kBit/s)
G.711	20	20	160	6	286	75%	114,4
G.711	30	30	240	6	366	50%	97,6
G.711	40	40	320	6	446	38%	89,2
G.711	60	60	480	6	606	25%	80,8
G.729A	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

Verschlüsselungs Algorithmus	Rahmengröße (ms)	Payload y (Bytes)	Padding x (Bytes)	Ethernet Paketlänge (Bytes)	Payload-Paket (Overhead in Prozent)	EthernetLoad (inkl. Header) (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 integrierte 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
- Android 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.

Tipp: 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.

19.3.3 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**.

19.3.4 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

IKE-SA

Payload-SA

Authentifizierung

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)

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.

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

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 konfiguriert. 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

Lightweight CA

CRL Certificate Revocation Lists - Zertifikatswiderrufslisten

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)

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.

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 widerrufenen 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.

19.3.6 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 Filialvernetzung 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 und Android VPN Client**

Das Betriebssystem iOS oder Android 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 vorgelegt.

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

Anmerkung: 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: **IP-Adresse/DynDNS-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

19.3.7 VPN - Dienste

Über die Funktion Konfigurierte Dienste können Sie Dienste verwalten. Konfigurierte Dienste werden erst durch Aktivieren zu aktiven Diensten.

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.

19.3.9 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.

19.3.10 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.

19.4 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.

CRL (Certificate Revocation Lists)

CDP (CRL Distribution Point)

Der Administrationszugriff erfolgt verschlüsselt über HTTPS unter Verwendung des TLS 1.2- 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.

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.

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.

Tipp: Die SSL-Zertifikatsgenerierung kann auch für SPE verwendet werden.

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 to go) zum internen Web-Server des Kommunikationssystems können entweder verschlüsselt (HTTPS) oder unverschlüsselt (HTTP) erfolgen.

Anmerkung: Unverschlüsselte Verbindungen zum Web-Server können Unbefugten den Zugriff auf sensible Daten ermöglichen! Aus Sicherheitsgründen wird dringend empfohlen, bei Nutzung von myPortal to go (Web Edition) über Internet nur eine verschlüsselte Verbindung (HTTPS) zu nutzen.

Für myPortal to go (App Edition) steht nur eine verschlüsselte Verbindung zum Web-Server zur Verfügung.

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.

19.6 SQL-Sicherheit

OpenScape Business speichert Systemkonfigurationsdaten, Anrufrdatensätze, Anmeldeinformationen für Benutzerkonten, UC-

Daten etc. in einer internen SQL-Datenbank. Der Zugriff auf die Datenbank wird über Login-Daten geschützt.

Bis SW-Version V2R2 waren die verwendeten Anmeldedaten durch ein Passwort geschützt, das vom OpenScape Business-Administrator nicht geändert werden konnte. Ab V2R2 ist das Passwort änderbar. Das Passwort wird maschinell generiert und ist für den Administrator nicht einsehbar. Um in Mehrfachknoten-Szenarien die Kompatibilität zu alten SW-Versionen zu gewährleisten, kann ein geändertes Passwort wieder auf den "alten" Wert zurückgesetzt werden. Die Konfiguration des SQL-Zugangskennworts erfolgt unter SQL-Sicherheit. Die Konfiguration des SQL-Zugangskennworts ist möglich in Netzwerkumgebungen und Einzelknoten-Umgebungen. Die Vorgehensweise für bestimmte Einzel- bzw. Mehrfachknoten-Szenarien wird in den nachfolgenden Kapiteln beschrieben.

19.6.1 Einzelknoten

SW-Upgrade von V2R1 oder älter

Nach einem SW-Upgrade von V2R1 ist das alte SQL-Datenbankkennwort aktiv. Das SQL-Kennwort muss in der neuen Software-Version vom Systemadministrator über das Administrationsportal (WBM) geändert werden.

Einrichtung des neuen Systems

Bei der Ersteinrichtung des Datums im System wird ein neues SQL-Kennwort generiert. Nur beim ersten Einstellen von Datum und Uhrzeit wird das SQL-Kennwort automatisch geändert.

Einrichtung eines neu geladenen "Einzelknotensystems"

Nach jedem Neuladen des Systems ist das alte SQL-Datenbankkennwort im System aktiv. Das SQL-Kennwort muss in der neuen Software-Version vom Systemadministrator über das Administrationsportal (WBM) geändert werden.

19.6.2 Mehrfachknoten

Das Einzelknotensystem wird mit der bereits bekannten Methode konfiguriert und in das Netzwerk integriert. Nach der Einrichtung des Systems synchronisiert der neue Slave-Knoten sein SQL-Kennwort mit dem Master-Knoten. Eine Anpassung des SQL-Kennworts innerhalb des Slave-Knotens ist nicht erforderlich.

Neuladen eines V2R2 oder höher Knotens in einem V2R2 oder höher Netzwerk

Nach dem Neuladen eines Netzwerkknotens in einem Netzwerk muss der Knoten neu konfiguriert und wieder in das Netzwerk integriert werden.

Neuladen des Master-Knotens

Bei einem Master-Knoten muss das SQL-Kennwort vom Systemadministrator über das Administrationsportal (WBM) geändert werden. Alle Slave-Knoten synchronisieren ihr SQL-Kennwort mit dem neuen Kennwort innerhalb des Master-Knotens. Eine Anpassung des SQL-Kennworts innerhalb der Slave-Knoten ist nicht erforderlich.

Neuladen des Slave-Knotens

Bei einem Slave-Knoten sind keine weiteren Maßnahmen erforderlich, da der Slave-Knoten sein SQL-Kennwort mit dem Master-Knoten synchronisiert.

Neuer V2R2 oder höher Slave-Knoten in einem V2R1-Netzwerk (Szenario wird nicht empfohlen)

Das Einzelknotensystem wird mit der bereits bekannten Methode konfiguriert und in das Netzwerk integriert. Nach der Einrichtung des Systems erkennt der neue Slave-Knoten, dass der Master-Knoten das alte SQL-Kennwort verwendet und verwendet dieses ebenfalls. Eine zusätzliche Anpassung des SQL-Kennworts innerhalb des Slave-Knotens ist nicht erforderlich.

Anmerkung: Es wird dringend empfohlen, das gesamte Netzwerk auf die letzte Softwareversion zu aktualisieren.

Neuer V2R2 oder höher Master-Knoten in einem V2R1-Netzwerk (Szenario wird nicht empfohlen)

Das Masterknotensystem wird mit der bereits bekannten Methode konfiguriert und in das Netzwerk integriert. Nach der Einrichtung des Systems verwendet der neue Master-Knoten das alte SQL-Kennwort. Der Systemadministrator darf das alte Kennwort nicht ändern, da die V2R1-Slaves keine Synchronisierung mit einem neuen SQL-Kennwort auf dem Master-Knoten durchführen können. In diesem Fall würde die Zusammenarbeit zwischen den Knoten innerhalb des Netzwerkes nicht funktionieren. Wenn der Systemadministrator das SQL-Kennwort versehentlich geändert hat, muss er dieses wieder auf das "Standardkennwort" der Masterknotenkonfiguration zurücksetzen.

Anmerkung: Es wird dringend empfohlen, das gesamte Netzwerk auf die letzte Softwareversion zu aktualisieren.

19.7 Schutz vor SIP-Attacken (SIP Attack Protection)

Sogenannte SIP-Attacken stellen eine neue Form der Angriffe auf Kommunikationsanlagen 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.

Tipp: 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 und OpenScape Business S Vernetzung (optional mit UC Suite oder UC Smart).
- OpenScape Business X mit OpenScape 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 **Vernetzungskonfiguration** 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), 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.

Tipp: 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 SIP-Q, lediglich TDM-Vernetzung auf Basis S_0/S_{2M} mit CorNet NQ wird unterstützt, siehe [Vernetzung über ISDN](#).
- HiPath 5000 RSM
- OpenScape Office MX

Vernetzung von OpenScape Business

Vernetzungsplan

- 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 Systeme) unterschieden.

Homogenes Netz (Natives Netzwerk)

Inhomogenes Netz (Hybrides Netzwerk)

Ein homogenes (natives) Netz besteht aus Komponenten der OpenScape Business Systemfamilie.

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 des WBM können alle OpenScape Business Knoten eines Netzverbundes angezeigt werden. Zusätzlich können auch alle OpenScape Business Teilnehmer des Netzverbundes nach Knoten sortiert angezeigt werden.

Folgende Informationen können 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)
- **Applikationsserver:** IP-Adresse des UC Servers (UC Booster Card oder UC Booster Server)
- **Registrierungsstatus:** Status der Registrierung
- **Aktiv:** Anzeige, ob der Knoten aktiv ist oder nicht

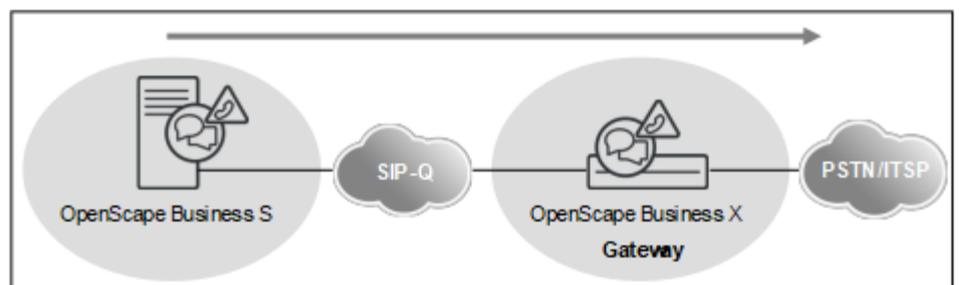
20.1.2 Single- und Multi-Gateway

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

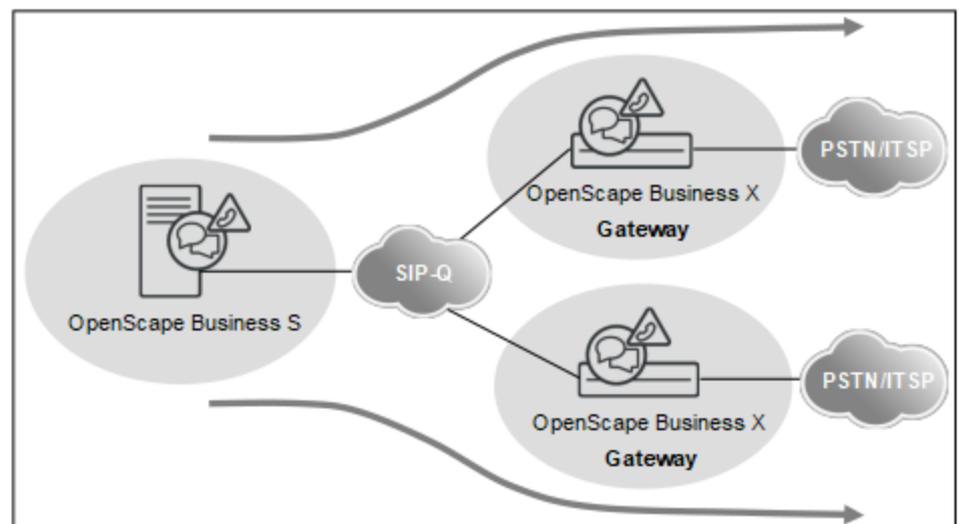
Multi-Gateway

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.

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 S) registriert.

Vernetzung von OpenScape Business

Netzweite Leistungsmerkmale

- 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-Lösung (UC Suite oder UC Smart) und deren UC Clients.

20.2.1 Netzweite Leistungsmerkmale der UC-Lösungen

Die folgende Tabelle bietet Ihnen einen Überblick über die netzweiten Leistungsmerkmale der beiden UC-Lösungen UC Smart und UC Suite.

Das UC-Interworking zur OpenScape 4000 und OpenScape Voice ist nicht möglich. In einem OpenScape Business Netzverbund sollte entweder UC Smart oder UC Suite verwendet werden. Gemischte UC-Lösungen werden nicht unterstützt.

Netzweite UC-Funktionen	UC Smart		UC Suite		
	myPortal @work	myPortal to go	myPortal for Desktop / Outlook	myPortal @work	myPortal to go
Netzweite Sichtbarkeit des Anwesenheitsstatus (Präsenz-Management)	x	x	x	x	x
Änderung des eigenen Anwesenheitsstatus über Client	x	x	x	x	x
Änderung des eigenen Anwesenheitsstatus über TUI	x	x	x	x	x
Statusbezogene Anrufumleitung	x	x	x	Über andere UC Suite Clients definierte Ziele	über myPortal definierte Ziele

Netzweite UC-Funktionen	UC Smart		UC Suite		
	myPortal @work	myPortal to go	myPortal for Desktop / Outlook	myPortal @work	myPortal to go
Netzweite Statusanzeige in Favoriten	x	x	x	x	x
Netzweite Statusanzeige in Verzeichnissen	x	x	x	x	x
Netzweite Statusanzeige im Journal	-	-	x	-	-
CallMe aktivieren	-	-	x	x	x
Kalender-Integration (Outlook)	-	-	x	-	-
Kalenderintegration (iCal) (nur mit myPortal for Desktop)	-	-	x	-	-
Netzweite Anzeige des Anrufstatus (Frei, Besetzt, Rufzustand)	x	x	x	x	x
Anlegen von Gruppen netzweit	x	x	x	-	-
Kompakte Anzeige der Favoriten	-	-	x	-	-
Gespräche	x	-	-	x	-
Persönliches Verzeichnis	Lokal	Lokal	Lokal	Lokal	Lokal
Internes Verzeichnis	Lokal	Lokal	Lokal	Lokal	Lokal
Externes Verzeichnis	-	-	x	x	x
Suche in Verzeichnissen netzweit	x	x	x	x	x
Zugriff auf im System definierte Kurzwahlziele (KWZ)	Lokal	Lokal	-	Lokal	Lokal
Import/Verwalten persönlicher Kontakte (CSV/XML)	x	-	x	-	-
Zugriff auf Outlook-Kontakte	x	-	x	-	-

Vernetzung von OpenScape Business

Netzweite UC-Funktionen	UC Smart		UC Suite		
	myPortal @work	myPortal to go	myPortal for Desktop / Outlook	myPortal @work	myPortal to go
Import von persönlichen Kontakten (Mac OS) (myPortal for Desktop)	-	-	X	-	-
Integration externer Verzeichnisse über LDAP	-	-	X	-	-
Alle Anrufe	X	X	X	X	X
Offene Anrufe	-	X	X	-	-
Entgangene Anrufe	X	X	X	X	X
Angenommene Anrufe	X	X	X	X	X
Geplante Anrufe	-	-	X	-	-
VoIP Anrufe	X	-	X	X	-
Fax-Journal	-	-	X	-	-
Manuelle Wahl	X	X	X	X	X
Desktop-Wahl (Click to Call)	-	-	X	-	-
Umleiten	X	X	X	X	X
Anruf halten	X	X	X	X	X
Aufzeichnen von Anrufen (Voice Recording)	-	-	X	-	-
E-Mail senden	X	X	X	X	X
SMS senden	-	X	-	-	X
Popups	X	-	X	X	-
AdHoc-Konferenz	X	X	X	X	X
Geplante Konferenzen	-	-	X	-	-
Permanente und offene Konferenzen (Drag&Drop-Konferenz)	X	-	X	-	-
Web Collaboration-Einbindung	X	-	X	X	-
Sprachbox (Visuelle Voicemail)	X	X	X	X	X
Sprachnachricht abhören über Telefon	X	X	X	X	X

Netzweite UC-Funktionen	UC Smart		UC Suite		
	myPortal @work	myPortal to go	myPortal for Desktop / Outlook	myPortal @work	myPortal to go
Sprachnachricht abhören über PC-Soundkarte	-	-	x	-	-
Senden einer Sprachnachricht als E-Mail	x	x	x	-	-
Fax (für Windows Betriebssysteme)	-	-	x	-	-
Instant Messaging (Chat) netzweit	x	-	x	-	-

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
Zweitenanruf	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
Rufweitchaltung im Besetztfall	Ja
Rufweitchaltung im Freifall	Ja
Call Deflection	Ja

Vernetzung von OpenScape Business

Lizenzierung eines Netzverbundes

Leistungsmerkmal	SIP-Q (IP-Netzwerk)
Advice of Charge at Call Setup	Nein
Advice of Charge during Call	Ja
Advice of Charge at the end of the call	Ja
Wegeoptimierung	Nein
Rerouting	Nein
Message Waiting Indication / Info	Ja
Fangen	Ja
Halten	Ja
Makeln	Ja
Übergabe	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.

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 hängen hierbei von der eingesetzten Netzwerktechnik ab.

Netzwerkparameter, Anforderung für LAN und WAN

Parameter	Mindestan	Hinweise
Delay (one way)	50 ms	Höhere Werte verschlechtern die Sprachqualität.
Round Trip Delay	100 ms	Höhere Werte verschlechtern die Sprachqualität.
Jitter	20 ms	Höhere Werte verschlechtern die Sprachqualität.
Packet Loss	3%	Bei Fax- oder Modem-Übertragungen über G.711 sollte der Paketverlust 0,05% nicht übersteigen (für den Fall, dass kein T.38 möglich ist).
Consecutive Packet Loss	3 bei G.711	Höhere Werte verschlechtern die Sprachqualität.

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 mindestens 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.

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	Paketierung Parameter	Sample Rate (ms)	Payload (Bytes)	Ethernet Paketlänge (Bytes)	Payload-Paket (Overhead in Prozent)	Ethernet Load (inkl. Header) (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:

	Sample Rate (ms)	Payload (Bytes)	Ethernet Paketlänge (Bytes)	Payload-Paket (Overhead in Prozent)	Ethernet Load (inkl. Header) (kBit/s)
T.38	30	169	227	34%	60,5

Payload-Verbindungen mit SRTP (Secure Realtime Transport Protocol) in einer LAN-Umgebung:

Codec-Typ	Sample Rate (ms)	Payload (Bytes)	Ethernet Paketlänge (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

Codec-Typ	Sample Rate (ms)	Payload (Bytes)	Ethernet Paketlänge (Bytes)	SRTP-Ethernet Paketlänge (kBit/s)	RTP-Ethernet Paketlänge (kBit/s)	Zusätzliche Bandbreite bei SRTP (%)
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 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.

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 10: 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.

Vernetzung von OpenScape Business

Wegeoptimierung (Path Replacement)

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:

- UC Smart
- UC Suite
- netzweiter CSP (CSTA Service Provider)
- DSS-Server
- CMD (CSTA Message Dispatcher)

Tabelle 11: Beispiele für offene Nummerierung

	Knoten 1	Knoten 2	Knoten 3	Knoten 4
Knotenrufnummer (Anlagenrufnummer)	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

20.4.2.1 Wahl von öffentlichen Rufnummern im Netz

Unabhängig von geschlossener oder offener Nummerierung 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.

Wenn mehrere OpenScape Business-Systeme vernetzt sind, kann z. B. folgendes Problem auftreten: Nehmen wir zunächst an, Teilnehmer A ruft Teilnehmer B an, der seinerseits alle Anrufe an Teilnehmer C umgeleitet hat. Die Teilnehmer A und C befinden sich im gleichen Netzknoten, aber Teilnehmer B befindet sich in 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.

Tipp: Das System-Flag für die Wegeoptimierung muss bei allen vernetzten OpenScape Business Systemen aktiviert werden!

: Es wird dringen empfohlen, die Funktion Wegeoptimierung nicht in Netzwerken zu verwenden, in denen analoge Faxstationen verwendet werden. Diese Einschränkung wird mit einer kommenden Softwareversion behoben.

Die Wegeoptimierung wird ausgeführt:

- Innerhalb des OpenScape Business Netzanteils
- Nach dem Verbindungsaufbau (nicht in der Rufphase!)
- Nach Transferszenarien
- Nach Rufweiserschaltung 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).

20.6 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 S in einer Hosting-Umgebung
- Vernetzung von OpenScape Business X und OpenScape 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

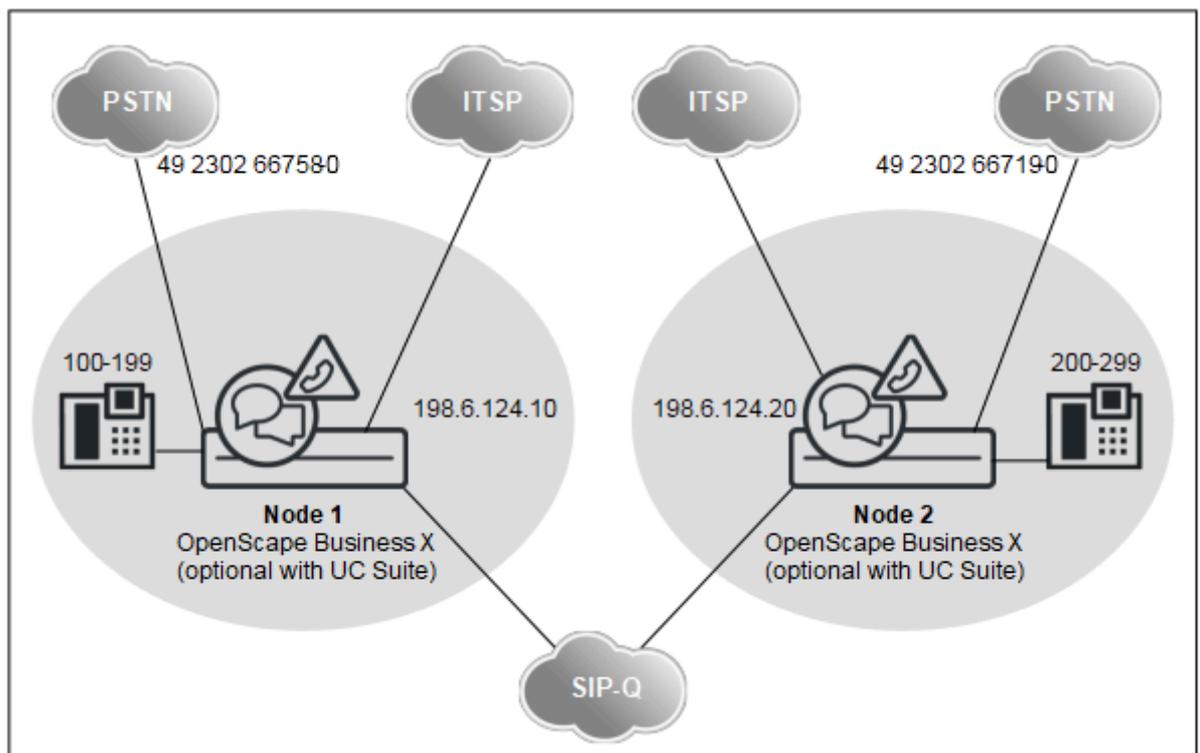
- Jedes System im Netzverbund ist einer eigenen Zeitzone zugeordnet. Alle Teilnehmer eines Systems haben daher dieselbe Zeitzone.
- OpenScape Business S Multi-Gateway-Vernetzungen sind nur innerhalb eines Landes (gleiche Zeitzone, gleiche Amtskennzahl) freigegeben.
- Generell wird jeder Netzverbund der OpenScape Business über Wizards konfiguriert. OpenScape Voice und OpenScape 4000 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, 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.
- In jedem Knoten kann nur EIN Voicemail-System zum Einsatz kommen. Generell sind in einem OpenScape Business Netzverbund verschiedenen Voicemail-Systeme erlaubt:
 - Kommt die UC Suite zum Einsatz, müssen andere im Netzverbund vorhandene Voicemail-Systeme vom Administrator deaktiviert werden.
 - Ein HiPath 3000 Netzverbund mit verschiedenen Voicemailsyste men kann 1:1 nach OpenScape Business migriert werden.
- Aus technischen Gründen können OpenScape Business X1-Systeme nicht als Master eingerichtet werden. Da in jedem OpenScape Business-Netzwerk ein Master-System erforderlich ist, muss mindestens ein System größer als X1 sein.

Tipp: 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 Vernetzung von mehreren OpenScape Business X

Bis zu 32 Kommunikationssysteme OpenScape Business X können miteinander vernetzt werden.

Netzwerkdaten



- Mit UC-Lösung (UC Smart oder UC Suite): nur geschlossene Nummerierung möglich
- Ohne UC-Lösung: geschlossene oder offene Nummerierung möglich
- Konfiguration über WBM (Wizards) bei geschlossener Nummerierung
- UC Suite Funktionalität basiert auf UC Booster Server oder UC Booster Card
- Bis zu 32 vernetzte Systeme und 1500 User ohne UC-Lösung
- Bis zu 8 vernetzte Systeme und 1500 User mit UC-Lösung

Netzweite Leistungsmerkmale

UC Vernetzung	Verdeckte (geschlossene) Nummerierung	Offene Nummerierung
Maximale Anzahl Knoten	8 mit UC-Lösung und 32 ohne UC-Lösung	

Vernetzung von OpenScape Business

UC Vernetzung	Verdeckte (geschlossene) Nummerierung	Offene Nummerierung
Maximale Anzahl von Teilnehmern in einem einzelnen Kommunikationssystem	abhängig von OpenScape Business X	
Maximale Anzahl von Teilnehmern im Netz	1500	

UC Vernetzung	Verdeckte (geschlossene) Nummerierung	Offene Nummerierung
UC Booster Card	UC Smart: 51 - 150 Teilnehmer (0 - 50 Teilnehmer ohne UC Booster Card) UC Suite: 0 - 150 Teilnehmer	Wird nicht unterstützt
UC Booster Server	UC Smart: ab 150 Teilnehmer UC Suite: ab 150 Teilnehmer	Wird nicht unterstützt

Administration	Verdeckte (geschlossene) Nummerierung	Offene Nummerierung
WBM	Netzweite Administration über Wizards	Netzweite Administration Expertenmodus
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	Verdeckte (geschlossene) Nummerierung	Offene Nummerierung
Lizenzierungsstruktur	Eine Vernetzungs-Lizenz für jeden Knoten erforderlich	

Konfiguration

Diese Konfiguration (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).

Tipp: 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.

Tabelle 12: 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	Leitungskennzahl	0
Vernetzung	2. AKZ	0
Richtungsparameter		
Richtung	Nr-Typ, gehend	RNR-Typ
Vernetzung	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.

Vernetzung von OpenScape Business

Tabelle 13: Übersicht der Einträge im LCR für Knoten 1

Rufnummernplan		Wegetabelle			Wahlregel		
Name	Gewählte Ziffern	Richtung	Dediziertes Gateway	Gateway ID	Wahlregel	Verfahren	Typ
Knoten 2 Internat	0C0049230266719-Z	Vernetzung	Erzwungen	2	D49230266719E3A	Corp. Network	International
Knoten 2 NAT	0C0230266719-Z						
Knoten 2 Teiln.	0C66719-Z						
Amt	0CZ	ISDN	Nein		A	Hauptnetzanbieter	Bekannt
Diverse	-Z	Vernetzung	Nein		A	Corp. Network	Unbekannt

Tabelle 14: 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	Leitungskennzahl	0
Vernetzung	2. AKZ	0
Richtungsparameter		
Richtung	Nr-Typ, gehend	RNR-Typ
Vernetzung	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.

Tabelle 15: Übersicht der Einträge im LCR für Knoten 2

Rufnummernplan		Wegetabelle			Wahlregel		
Name	Gewählte Ziffern	Richtung	Dediziertes Gateway	Gateway ID	Wahlregel	Verfahren	Typ
Knoten 1 Internat	0C0049230266758-Z	Vernetzung	Erzwungen	1	D49230266758E3A	Corp. Network	International

Rufnummernplan		Wegetabelle			Wahlregel		
Name	Gewählte Ziffern	Richtung	Dediziertes Gateway	Gateway ID	Wahlregel	Verfahren	Typ
Knoten 1 NAT	0C0230266758-Z						
Knoten 1 Teiln.	0C66758-Z						
Amt	0CZ	ISDN	Nein		A	Hauptnetzanbieter	Bekannt
Diverse	-Z	Vernetzung	Nein		A	Corp. Network	Unbekannt

Vorgehensweise bei der Einrichtung der Vernetzung:

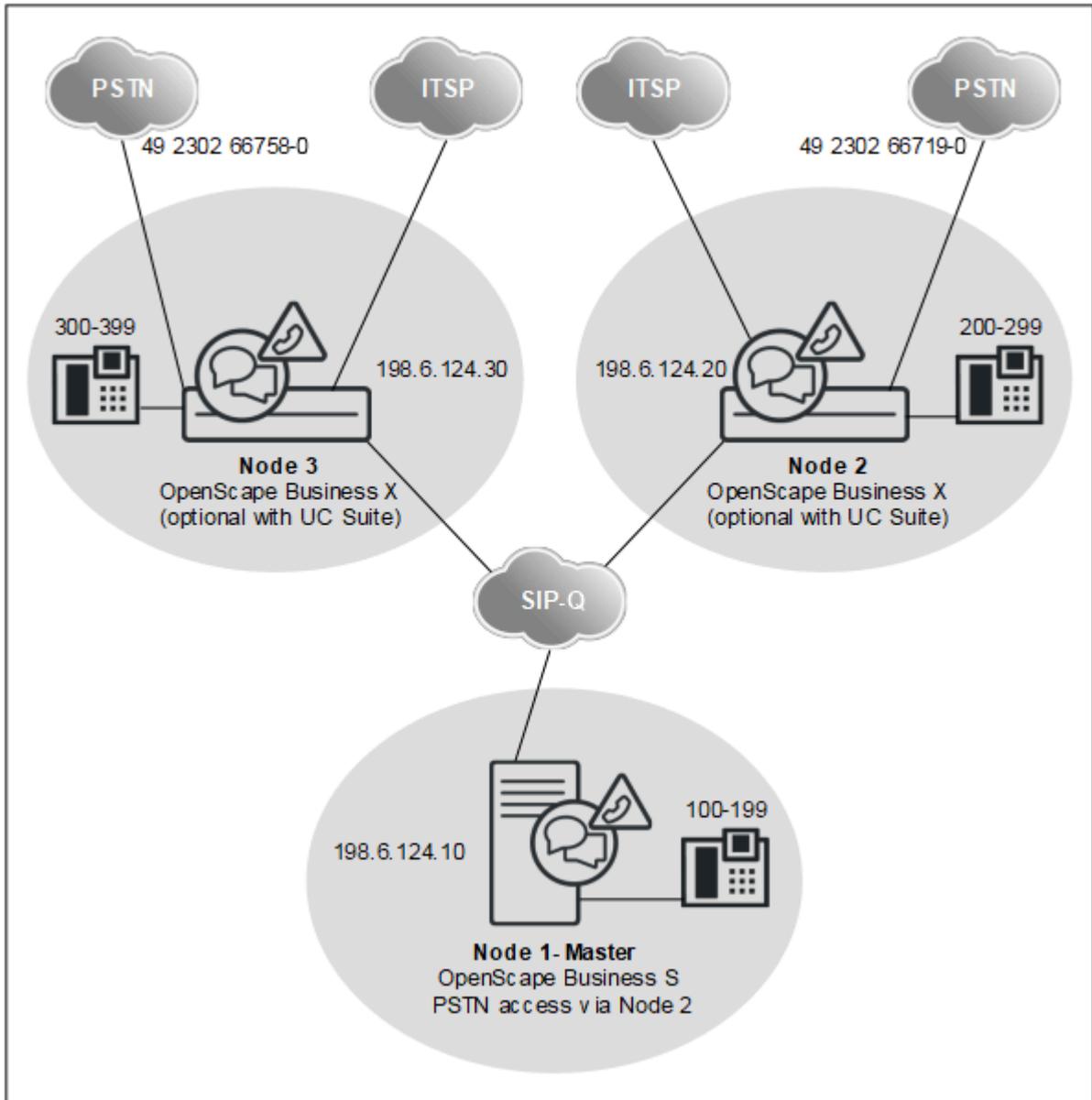
- 1)** Basisinstallation für Knoten 1 (Master) konfigurieren
- 2)** Vernetzung konfigurieren für Knoten 1
- 3)** Basisinstallation für Knoten 2 (Slave) konfigurieren
- 4)** Vernetzung konfigurieren für Knoten 2
- 5)** Vernetzungsfunktion kontrollieren für Master
- 6)** Richtungen und Richtungsparameter 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)

20.6.3 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 oder ITSP verwenden.

Vernetzung von OpenScape Business

Netzwerkdaten



- Verdeckte (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
- Es sind mehrere OpenScape Business S im Netzverbund erlaubt.
- Bis zu 32 vernetzte Systeme und 1500 User ohne UC-Lösung
- Bis zu 8 vernetzte Systeme und 1500 User mit UC-Lösung

Netzweite Leistungsmerkmale

UC Vernetzung	Verdeckte (geschlossene) Nummerierung	Offene Nummerierung
Maximale Anzahl Knoten	8 mit UC-Lösung und 32 ohne UC-Lösung	

UC Vernetzung	Verdeckte (geschlossene) Nummerierung	Offene Nummerierung
Maximale Anzahl von Teilnehmern in einem einzelnen Kommunikationssystem	abhängig von OpenScape Business X	
Maximale Anzahl von Teilnehmern im Netz	1500	

UC Vernetzung	Verdeckte (geschlossene) Nummerierung	Offene Nummerierung
UC Booster Card	UC Smart: 51 - 150 Teilnehmer (0 - 50 Teilnehmer ohne UC Booster Card) UC Suite: 0 - 150 Teilnehmer	Wird nicht unterstützt
UC Booster Server	UC Smart: ab 150 Teilnehmer UC Suite: ab 150 Teilnehmer	Wird nicht unterstützt

Administration	Verdeckte (geschlossene) Nummerierung	Offene Nummerierung
WBM	Netzweite Administration über Wizards	Wird nicht unterstützt
Manager E	Netzweite Administration für spezielle Aufgaben (nicht für OpenScape Business S)	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	Verdeckte (geschlossene) Nummerierung	Offene Nummerierung
Lizenzierungsstruktur	Eine Vernetzungs-Lizenz für jeden Knoten erforderlich	Wird nicht unterstützt

Konfiguration

Diese Konfiguration (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-

Vernetzung von OpenScape Business

Rufnummern dürfen mehrfach vorkommen (z.B. Amtsrufnummer 49 2302 66758 100 und 49 2302 66719 100 haben dieselbe 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.

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.

Tabelle 16: Einrichtung der Standortdaten für Knoten 1 OpenScape Business S

Knoten 1		
G.-Standort Land		49
G.-Standort Ortsnetz		2302
G.-Standort Anlage		66719
Internationales Präfix		00
Nationales Präfix		0
Richtungen		
Rtg. 1	Leitungskennzahl	0
Vernetzung	2. AKZ	0
Richtungsparameter		
Richtung	Nr-Typ, gehend	RNR-Typ
Vernetzung	Unbekannt	Int/Duwa

Knoten 1		
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.

Tabelle 17: Übersicht der Einträge im LCR für Knoten 1

Rufnummernplan		Wegetabelle			Wahlregel		
Name	Gewählte Ziffern	Richtung	Dediziertes Gateway	Gateway ID	Wahlregel	Verfahren	Typ
Knoten 2 Internat	0C0049230266719-2Z	Vernetzung	Erzwungen	2	D49230266719E3A	Corp. Network	International
Knoten 2 NAT	0C0230266719-2Z						
Knoten 2 Teiln.	0C66719-2Z						
Knoten 3 Internat	0C0049230266758-3Z	Vernetzung	Erzwungen	3	D49230266758E3A	Corp. Network	International
Knoten 3 NAT	0C0230266758-3Z						
Knoten 3 Teiln.	0C66758-3Z						
Amt	0CZ	Vernetzung	Erzwungen	2	E1A	Hauptnetzanbieter	Bekannt
Diverse	-Z	Vernetzung	Nein		A	Corp. Network	Unbekannt

Tabelle 18: Einrichtung der Standortdaten für Knoten 2 OpenScape Business

Knoten 2		
G.-Standort Land		49
G.-Standort Ortsnetz		2302
G.-Standort Anlage		66719
Internationales Präfix		00
Nationales Präfix		0
Richtungen		
ISDN	Leitungskennzahl	0
Vernetzung	2. AKZ	0
Richtungsparameter		
Richtung	Nr-Typ, gehend	RNR-Typ

Vernetzung von OpenScape Business

Knoten 2		
Vernetzung	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.

Tabelle 19: Übersicht der Einträge im LCR für Knoten 2

Rufnummernplan		Wegetabelle			Wahlregel		
Name	Gewählte Ziffern	Richtung	Dediziertes Gateway	Gateway ID	Wahlregel	Verfahren	Typ
Knoten 1 Internat	0C0049230266719-1Z	Vernetzung	Erzwungen	1	D49230266719E3A	Corp. Network	International
Knoten 1 NAT	0C0230266719-1Z						
Knoten 1 Teiln.	0C66719-1Z						
Knoten 3 Internat	0C0049230266758-3Z	Vernetzung	Erzwungen	3	D49230266758E3A	Corp. Network	International
Knoten 3 NAT	0C0230266758-3Z						
Knoten 3 Teiln.	0C66758-3Z						
Amt	0CZ	ISDN	Nein		A	Hauptnetzanbieter	Unbekannt
Diverse	-Z	Vernetzung	Nein		A	Corp. Network	Unbekannt

Tabelle 20: Einrichtung der Standortdaten für Knoten 3 OpenScape Business

Knoten 3		
G.-Standort Land		49
G.-Standort Ortsnetz		2302
G.-Standort Anlage		66758
Internationales Präfix		00
Nationales Präfix		0
Richtungen		
ISDN	Leitungskennzahl	0
Vernetzung	2. AKZ	0
Richtungsparameter		

Knoten 3		
Richtung	Nr-Typ, gehend	RNR-Typ
Vernetzung	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.

Tabelle 21: Übersicht der Einträge im LCR für Knoten 3

Rufnummernplan		Wegetabelle			Wahlregel		
Name	Gewählte Ziffern	Richtung	Dediziertes Gateway	Gateway ID	Wahlregel	Verfahren	Typ
Knoten 1 Internat	0C0049230266719-1Z	Vernetzung	Erzwungen	1	D49230266719E3A	Corp. Network	International
Knoten 1 NAT	0C0230266719-1Z						
Knoten 1 Teiln.	0C66719-1Z						
Knoten 2 Internat	0C0049230266719-2Z	Vernetzung	Erzwungen	2	D49230266719E3A	Corp. Network	International
Knoten 2 NAT	0C0230266719-2Z						
Knoten 2 Teiln.	0C66719-2Z						
Amt	0CZ	ISDN	Nein		A	Hauptnetzanbieter	Unbekannt
Diverse	-Z	Vernetzung	Nein		A	Corp. Network	Unbekannt

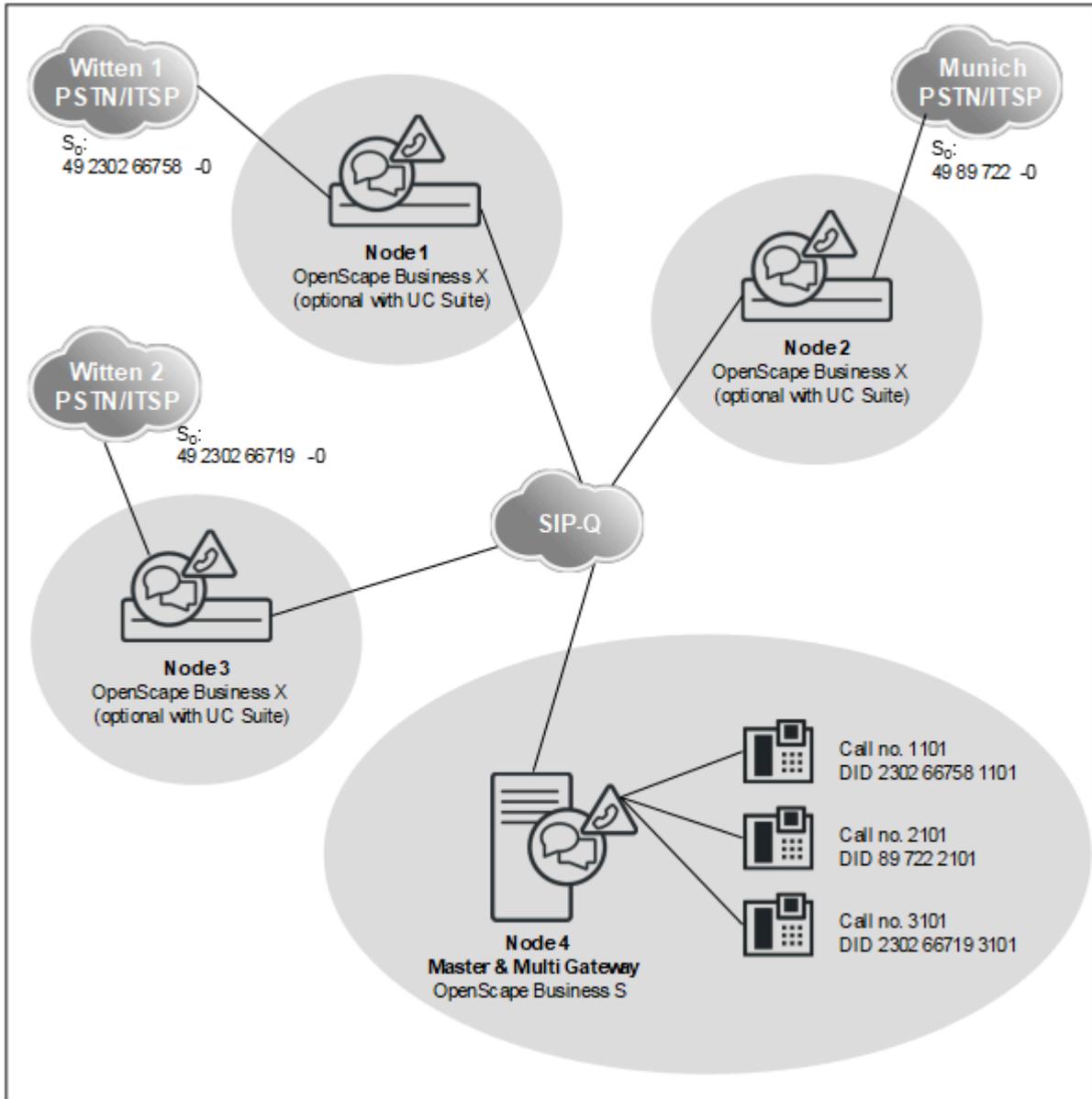
Vorgehensweise bei der Einrichtung der Vernetzung:

- 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)

20.6.4 Vernetzung von Open Scape Business X und OpenScape Business S (Multi Gateway)

Bis zu 32 Kommunikationssysteme OpenScape Business X und OpenScape Business S können miteinander vernetzt werden. Multi Gateway bedeutet, dass jeder an OpenScape Business S registrierte IP-Teilnehmer genau einem bestimmten Gateway zugeordnet sind.

Netzwerkdaten



- Verdeckte (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

- 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 und 1500 User ohne UC-Lösung
- Bis zu 8 vernetzte Systeme und 1500 User mit UC-Lösung

Netzweite Leistungsmerkmale

UC Vernetzung	Verdeckte (geschlossene) Nummerierung	Offene Nummerierung
Maximale Anzahl Knoten	8 mit UC-Lösung und 32 ohne UC-Lösung	
Maximale Anzahl von Teilnehmern in einem einzelnen Kommunikationssystem	abhängig von OpenScape Business X	
Maximale Anzahl von Teilnehmern im Netz	1500	

UC Vernetzung	Verdeckte (geschlossene) Nummerierung	Offene Nummerierung
UC Booster Card	UC Smart: 51 - 150 Teilnehmer (0 - 50 Teilnehmer ohne UC Booster Card) UC Suite: 0 - 150 Teilnehmer	Wird nicht unterstützt
UC Booster Server	UC Smart: ab 150 Teilnehmer UC Suite: ab 150 Teilnehmer	Wird nicht unterstützt

Administration	Verdeckte (geschlossene) Nummerierung	Offene Nummerierung
WBM	Netzweite Administration über Wizards	Wird nicht unterstützt
Manager E	Netzweite Administration für spezielle Aufgaben (nicht für OpenScape Business S)	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

Vernetzung von OpenScape Business

Lizenzierung	Verdeckte (geschlossene) Nummerierung	Offene Nummerierung
Lizenzierungsstruktur	Eine Vernetzungs-Lizenz für jeden Knoten erforderlich	Wird nicht unterstützt

Konfiguration

Diese Konfiguration (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 (geschlossener) Nummerierung nur einmal vergeben ist. Unterschiedliche Rufnummerlängen 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.

Tabelle 22: 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	Leitungskennzahl	0
Vernetzung	2. AKZ	0
Richtungsparameter		
Richtung	Nr-Typ, gehend	RNR-Typ
Vernetzung	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.

Tabelle 23: Übersicht der Einträge im LCR für Knoten 1

Rufnummernplan		Wegetabelle			Wahlregel		
Name	Gewählte Ziffern	Richtung	Dediziertes Gateway	Gateway ID	Wahlregel	Verfahren	Typ
Knoten 2 Internat	0C004989722-Z	Vernetzung	Erzwungen	2	D4989722E3A	Corp. Network	International
Knoten 2 NAT	0C089722-Z						
Knoten 2 Teiln.	0C722-Z						
Knoten 3 Internat	0C0049230266719-Z	Vernetzung	Erzwungen	3	D49230266719E3A	Corp. Network	International
Knoten 3 NAT	0C0230266719-Z						
Knoten 3 Teiln.	0C66719-Z						
Knoten 4 Internat	0C0049230266758-Z	Vernetzung	NEIN		D230266758E3A	Corp. Network	National
Knoten 4 NAT	0C0230266758-Z						
Knoten 4 Teiln.	0C66758-Z						
Diverse	-Z	Vernetzung	Nein		BA	Corp. Network	Unbekannt
Amt International	0C0049-Z	ISDN	Nein		D0E3A	Hauptnetzanbieter	Unbekannt
Amt	0CZ	ISDN	Nein		A	Hauptnetzanbieter	Unbekannt

Tabelle 24: Einrichtung der Standortdaten für Knoten 2

Knoten 2		
G.-Standort Land		49
G.-Standort Ortsnetz		89
G.-Standort Anlage		722
Internationales Präfix		00
Nationales Präfix		0
Richtungen		
ISDN	Leitungskennzahl	0
Vernetzung	2. AKZ	0

Vernetzung von OpenScape Business

Knoten 2		
Richtungsparameter		
Richtung	Nr-Typ, gehend	RNR-Typ
Vernetzung	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.

Tabelle 25: Übersicht der Einträge im LCR für Knoten 2

Rufnummernplan		Wegetabelle			Wahlregel		
Name	Gewählte Ziffern	Richtung	Dediziertes Gateway	Gateway ID	Wahlregel	Verfahren	Typ
Knoten 1 Internat	0C0049230266758-Z	Vernetzung	Erzwungen	1	D492302667E3A	Corp. Network	International
Knoten 1 NAT	0C0230266758-Z						
Knoten 1 Teiln.	0C66758-Z						
Knoten 3 Internat	0C0049230266719-Z	Vernetzung	Erzwungen	3	D49230266719E3A	Corp. Network	International
Knoten 3 NAT	0C0230266719-Z						
Knoten 3 Teiln.	0C66719-Z						
Knoten 4 Internat	0C004989722-Z	Vernetzung	NO		D89722E3A	Corp. Network	National
Knoten 4 NAT	0C089722-Z						
Knoten 4 Teiln.	0C722-Z						
Diverse	-Z	Vernetzung	Nein		BA	Corp. Network	Unbekannt
Amt International	0C0049-Z	ISDN	Nein		D0E3A	Hauptnetzanbieter	Unbekannt
Amt	0CZ	ISDN	Nein		A	Hauptnetzanbieter	Unbekannt

Tabelle 26: Einrichtung der Standortdaten für Knoten 3

Knoten 3	
G.-Standort Land	49

Knoten 3		
G.-Standort Ortsnetz		2302
G.-Standort Anlage		66719
Internationales Präfix		00
Nationales Präfix		0
Richtungen		
ISDN	Leitungskennzahl	0
Vernetzung	2. AKZ	0
Richtungsparameter		
Richtung	Nr-Typ, gehend	RNR-Typ
Vernetzung	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.

Tabelle 27: Übersicht der Einträge im LCR für Knoten 3

Rufnummernplan		Wegetabelle			Wahlregel		
Name	Gewählte Ziffern	Richtung	Dediziertes Gateway	Gateway ID	Wahlregel	Verfahren	Typ
Knoten 1 Internat	0C0049230266758-Z	Vernetzung	Erzwungen	1	D49230266758E3A	Corp. Network	International
Knoten 1 NAT	0C0230266758-Z						
Knoten 1 Teiln.	0C66758-Z						
Knoten 2 Internat	0C004989722-Z	Vernetzung	Erzwungen	2	D4989722E3A	Corp. Network	International
Knoten 2 NAT	0C089722-Z						
Knoten 2 Teiln.	0C722-Z						
Knoten 4 Internat	0C004989230266719-Z	Vernetzung	Nein		D230266719E3A	Corp. Network	National
Knoten 4 NAT	0C0230266719-Z						
Knoten 4 Teiln.	0C66719-Z						
Diverse	-Z	Vernetzung	Nein		BA	Corp. Network	Unbekannt

Vernetzung von OpenScape Business

Rufnummernplan		Wegetabelle			Wahlregel		
Name	Gewählte Ziffern	Richtung	Dediziertes Gateway	Gateway ID	Wahlregel	Verfahren	Typ
Amt International	0C0049-Z	ISDN	Nein		D0E3A	Hauptnetzanbieter	Unbekannt
Amt	0CZ	ISDN	Nein		A	Hauptnetzanbieter	Unbekannt

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.

Tabelle 28: Knoten 4, Pseudo-Amtsrichtung

Knoten 4		
G.-Standort Land		49
G.-Standort Ortsnetz		
G.-Standort Anlage		
Internationales Präfix		00
Nationales Präfix		0
Richtungen		
ISDN	Leitungskennzahl	0
Vernetzung	2. AKZ	0
Richtungsparameter		
Richtung	Nr-Typ, gehend	RNR-Typ
Vernetzung	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.

Tabelle 29: Knoten 4, Richtung Networking

Knoten 4		
G.-Standort Land		
G.-Standort Ortsnetz		
G.-Standort Anlage		
Internationales Präfix		00
Nationales Präfix		0
Richtungen		
ISDN	Leitungskennzahl	0

Knoten 4		
Vernetzung	2. AKZ	0
Richtungsparameter		
Richtung	Nr-Typ, gehend	RNR-Typ
Vernetzung	National	Int/Duwa
ISDN	(Keine Änderung des Eintrags)	DuWa

Tabelle 30: Übersicht der Einträge im LCR für Knoten 4

Rufnummernplan		Wegetabelle			Wahlregel		
Name	Gewählte Ziffern	Richtung	Dediziertes Gateway	Gateway ID	Wahlregel	Verfahren	Typ
Knoten 1 Internat	0C0049230266758-Z	Vernetzung	Erzwungen	1	D49230266758E3A	Corp. Network	International
Knoten 1 NAT	0C0230266758-Z						
Knoten 2 Internat	0C004989722-Z	Vernetzung	Erzwungen	2	D4989722E3A	Corp. Network	International
Knoten 2 NAT	0C089722-Z						
Knoten 3 Internat	0C004989230266719-Z	Vernetzung	Erzwungen	3	D49230266719E3A	Corp. Network	International
Knoten 3 NAT	0C0230266719-Z						
Diverse	-Z	Vernetzung	NEIN		A	Corp. Network	Unbekannt
Amt	0CZ	Vernetzung	MULTI-GATEWAY	1	E1A	Hauptnetzanbieter	Unbekannt

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 für Knoten 2 konfigurieren (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)

20.6.5 Vernetzung von OpenScape Business in Hosting-Umgebungen

In einer Umgebung mit mehreren Standorten (Hosting-Umgebung) kann jedem Standort eine Richtung und jeder Richtung eine ITSP-Registrierung zugeordnet werden. Es können max. 8 ITSP-Registrierungen verwaltet werden. Dabei ist eine Registrierung pro ITSP möglich oder auch mehrere Registrierungen an einem ITSP. Jeder ITSP-Registrierung kann eine Ortsvorwahl und anschließend mehrere Teilnehmer zugeordnet werden. Der Anschluss der Teilnehmer an den verschiedenen Standorten an das Kommunikationssystem erfolgt über VPN oder MPLS. Befinden sich die Standorte in unterschiedlichen Ländern, ist für jedes Land eine eigene OpenScape Business S zu verwenden (Szenario 1a). Befinden sich alle Standorte innerhalb eines Landes, kann eine OpenScape Business S verwendet werden (Szenario 1b).

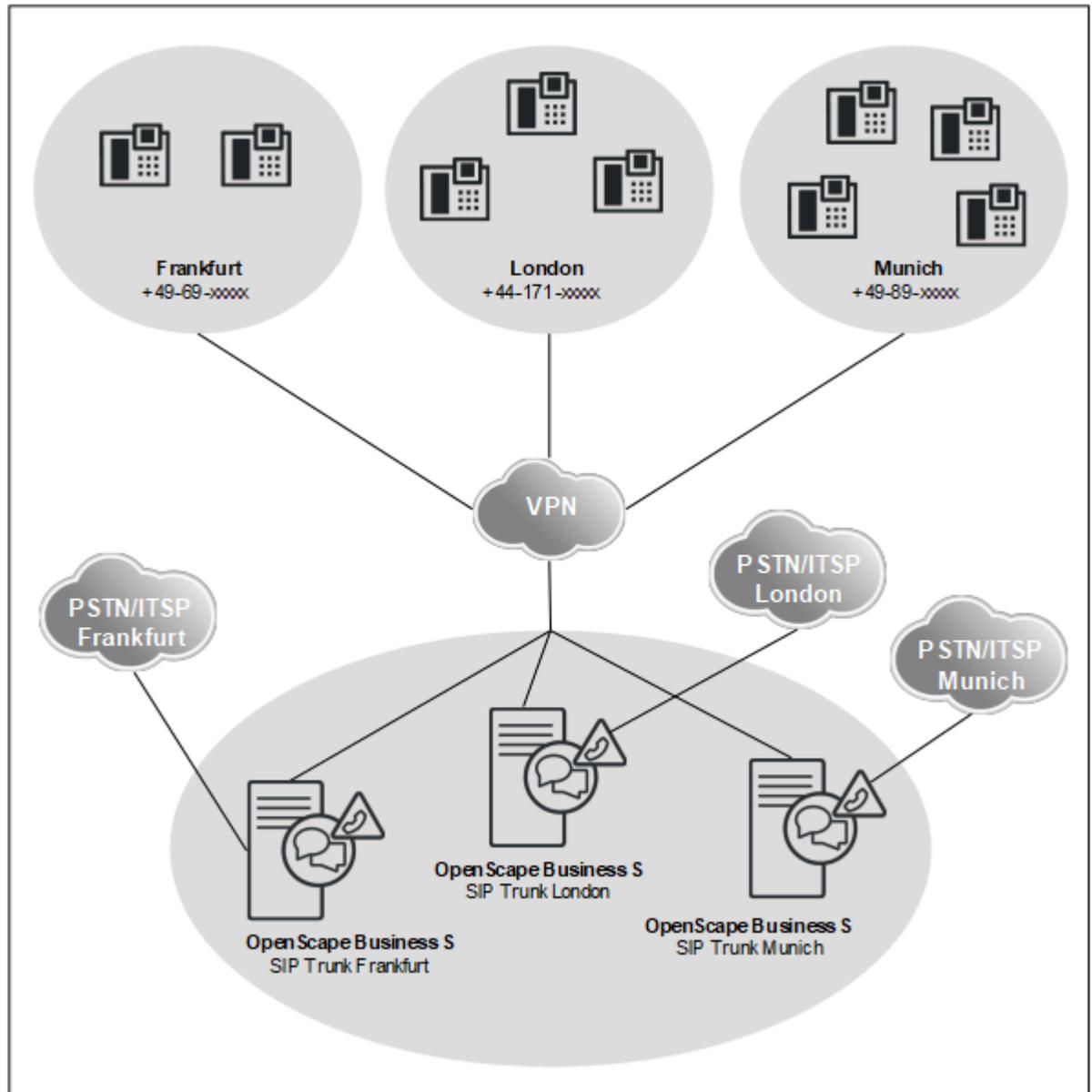
Beide Szenarien sind auch mit den OpenScape Business X Hardwaremodellen realisierbar (z.B. bei kleinen Ausbauten). An einem Standort lassen sich zusätzlich die TDM-Komponenten mit nutzen.

Die nachfolgend genannten Hosting-Szenarien sind allgemein beschrieben. Folgende Ausprägungen sind realisierbar:

- Einsatz von OpenScape Business S und OpenScape Business X im Datacenter des Kunden bzw. beim Hoster
- OpenScape Business S auf dedizierter Server-Hardware oder virtualisiert
- Voraussetzung ist eine VPN-oder MPLS-Infrastruktur, insbesondere bei mehreren Kunden-Standorten (keine standortspezifischen NAT-Router als Internetzugang)
- Bis zu 8 ITSP je System und Land, MSN- oder Durchwahl-Provider
- Bis zu 8 Standort-Vorwahlen (Area Codes) je System und Land, zugeordnet zu bis zu 8 Kunden-Standorten (Multi-Site)
- Multi-Site-Szenarien kombinierbar mit klassischer Vernetzung (Voice und UC)
- Multi-Site >8 Standorte in Vernetzungen realisierbar (n-mal Multi-Site vernetzt)
- Multi-Site länderübergreifend in Vernetzungen realisierbar (n-mal Multi-Site vernetzt)
- Vernetzungsszenarien mit ISDN-Gateways voll integrierbar
- Technische Voraussetzung ist die Möglichkeit, Durchwahlruffnummern für ISDN-Provider wie für SIP-Provider gleichermaßen zu verwenden.

Szenario a: Hosting mit einer OpenScape Business S pro Standort

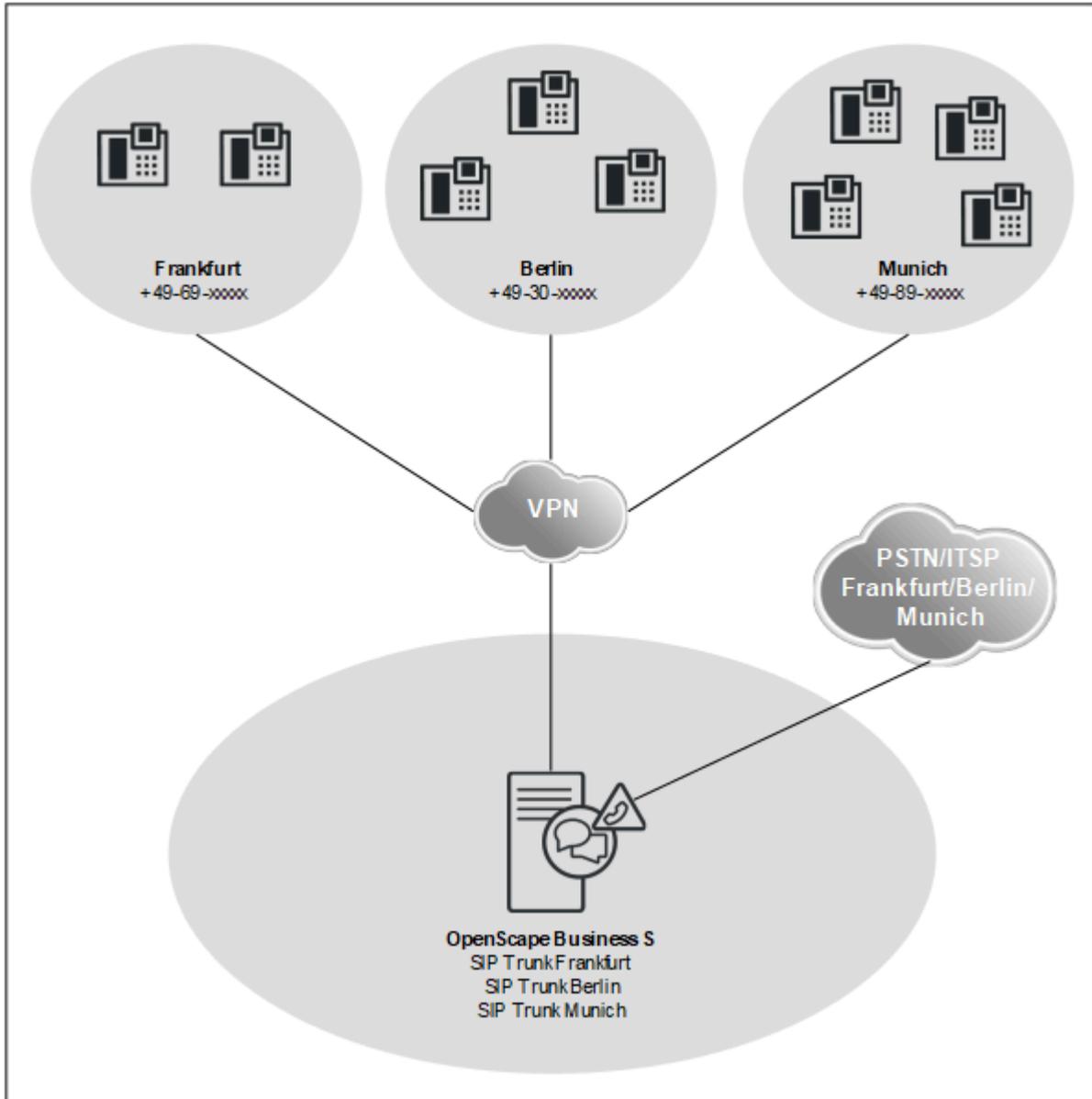
Netzwerkdaten



- Ein Kunde innerhalb eines VPN oder MPLS.
- Eine OpenScape Business S pro Standort.
- Standorte können innerhalb eines Landes oder über mehrere Länder verteilt sein.
- Bis zu 1000 User und 180 SIP-Trunks pro OpenScape Business S.
- OpenScape Business Vernetzung optional, bis zu insg. 1500 User. Größere Ausbauten sind im Rahmen von projektspezifischen Freigaben möglich.

Szenario b: Hosting mit einer OpenScape Business S für mehrere Standorte

Netzwerkdaten



- Ein Kunde innerhalb eines VPN oder MPLS.
- Eine OpenScape Business S für alle Standorte.
- Standorte nur innerhalb eines Landes.
- Bis zu 8 Standorte mit unterschiedlichen Standortvorwahlen.
- Bis zu 8 SIP-Provider pro OpenScape Business S.
- Ein SIP-Provider pro Standort.
- Bis zu 1000 User und 180 SIP-Trunks.
- OpenScape Business Vernetzung mit mehreren OpenScape Business S innerhalb eines VPN optional (OS Biz S 1 in Land 1, OS Biz S 2 in Land 2, usw.), bis zu insg. 1500 User. Größere Ausbauten sind im Rahmen von projektspezifischen Freigaben möglich.

- Konfigurationsbeispiel siehe Unify Experts Wiki im Internet unter *ITSP Configuration Guide*.

20.6.6 Vernetzung von OpenScape Business X und OpenScape 4000

Eine Vernetzung von OpenScape Business X mit OpenScape 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 (Szenario 4b).

Anmerkung: 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

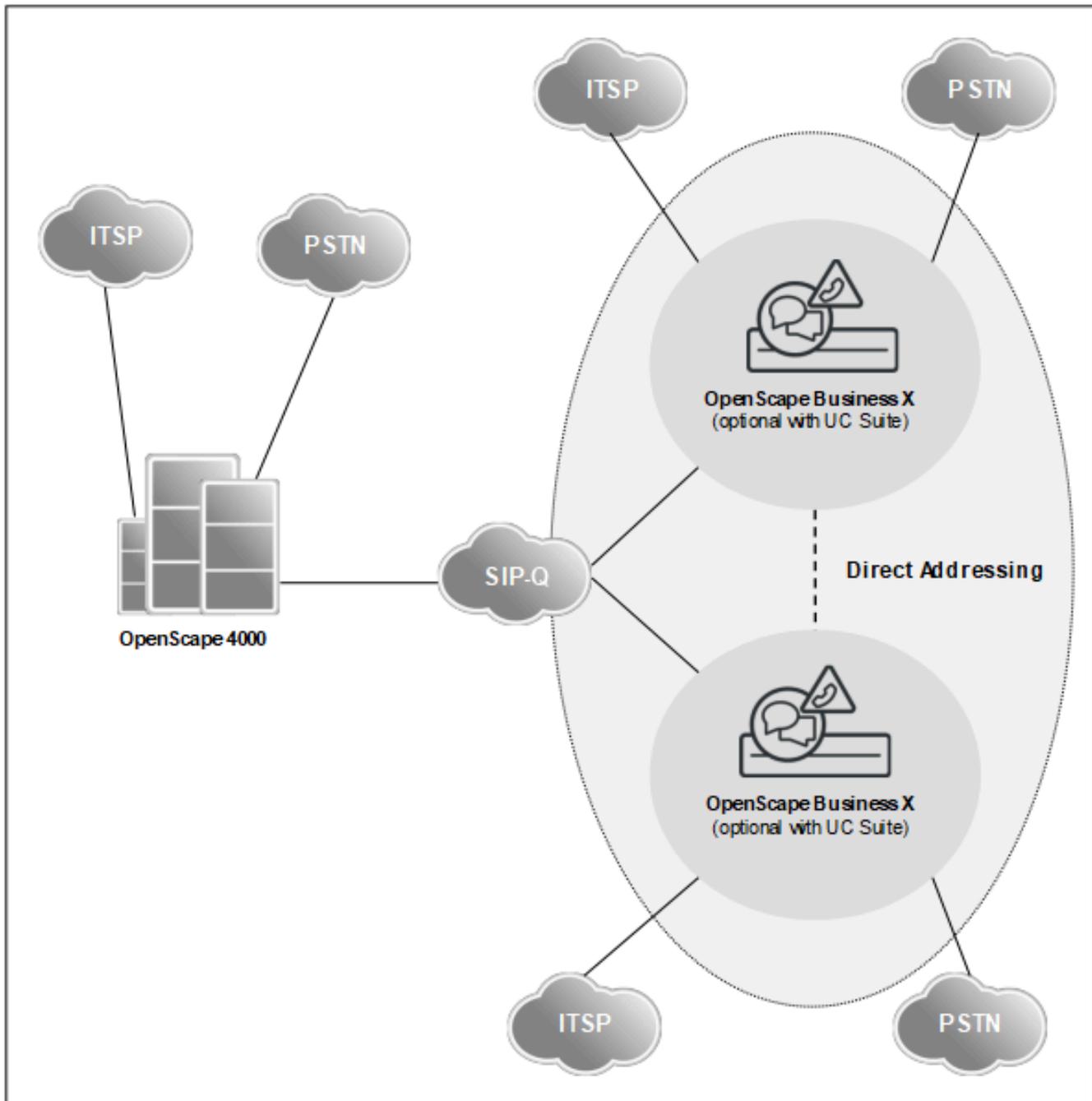
Vernetzung von OpenScape Business

Szenario a: Netzverbund mit OpenScape 4000 und direkter Adressierung zwischen den OpenScape Business X Knoten

Netzwerkdaten

Szenario b: Netzverbund mit OpenScape 4000 und Routing aller Verbindungen über OpenScape 4000

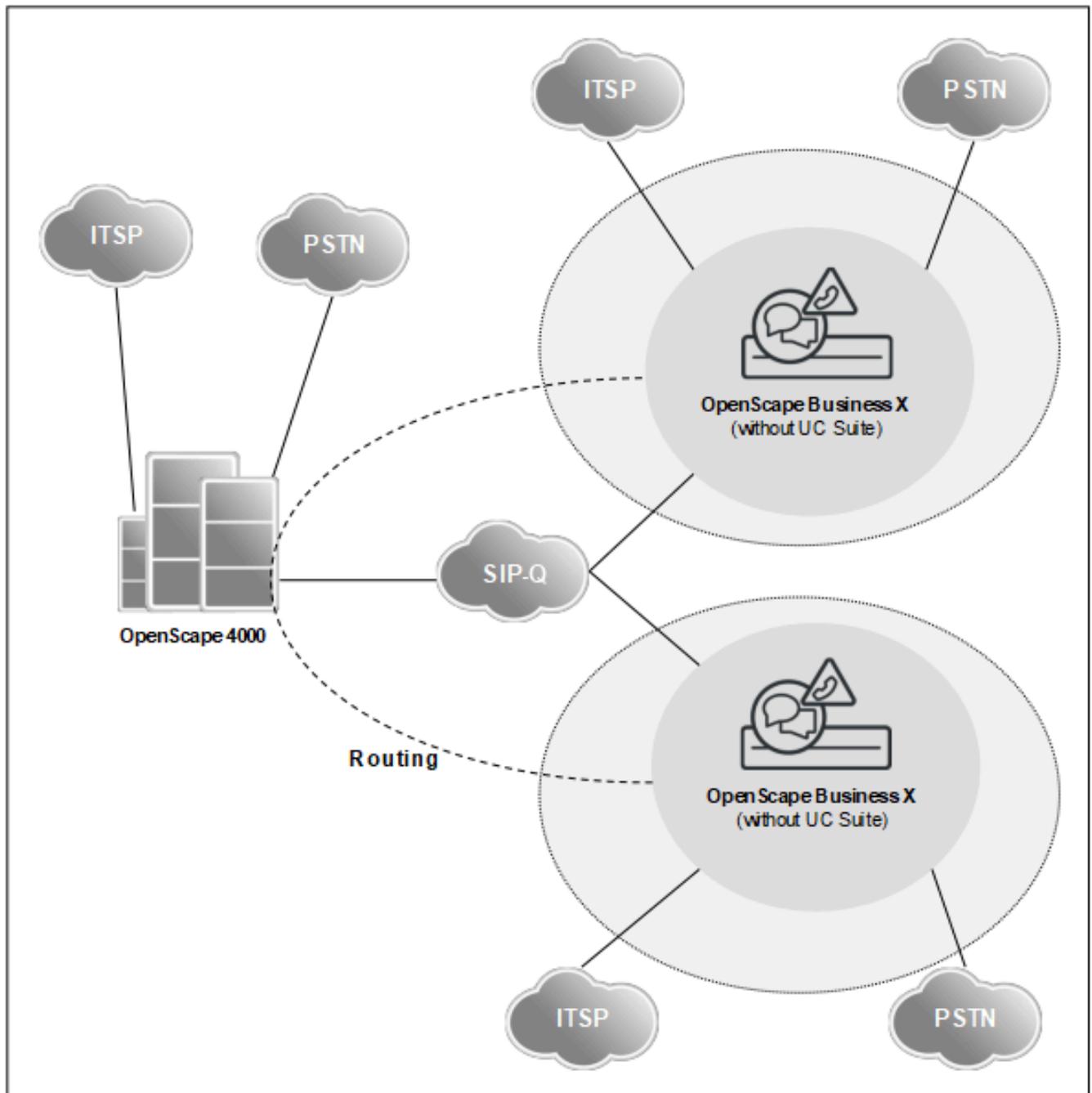
Netzwerkdaten



- Geschlossene Nummerierung innerhalb der OpenScape Business Vernetzung

Vernetzung von OpenScape Business

- Netzweite Sprach- und UC-Funktionalität innerhalb der OpenScape Business Vernetzung
- Konfiguration über den Assistenten "Vernetzung" für die OpenScape Business Vernetzung
- Konfiguration der OpenScape 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.



- Offene Nummerierung

Vernetzung von OpenScape Business

- Netzweite Sprach-Funktionalität
- Jedes Gespräch in einen anderen Knoten wird über OpenScape 4000 geroutet
- Keine UC-Lösung 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

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)	
Maximale Anzahl von Teilnehmern pro System	Abhängig vom OpenScape Business X Modell	
Maximale Anzahl von Teilnehmern im Netz	1500 für den OpenScape Business Netz-Anteil	Abhängig von OpenScape 4000
Sprachvernetzung	SIP-Q	

UC Vernetzung	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
	Netzweite Funktionalität innerhalb der OpenScape Business	Nicht unterstützt
UC Booster Card	UC Smart: 51 - 150 Teilnehmer (0 - 50 Teilnehmer ohne UC Booster Card) UC Suite 0 - 150 Teilnehmer	Nicht unterstützt
UC Booster Server	UC Smart: ab 150 Teilnehmer UC Suite: ab 150 Teilnehmer	Nicht unterstützt
OpenScape Business S	Unterstützt	Nicht unterstützt

Administration	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
	WBM mit Wizards für OpenScape Business Knoten, OpenScape 4000 wird über Expertenmodus der OpenScape Business administriert	Netzweite Administration Expertenmodus
WBM	WBM mit Wizards	WBM mit Expertenmodus

Administration	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
Manager E	Nicht empfohlen	Nicht empfohlen
UC-Suite-Administration	WBM mit Wizards für OpenScape Business Knoten	Nicht unterstützt
Massendatenimport über csv-Dateien (Rufnummern, Durchwahlnummern, Namen)	Separat für jeden Knoten im Netzverbund	

Lizenzierung	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
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	Nicht unterstützt
Sofortnachricht versenden	Netzweit, innerhalb der OpenScape Business Vernetzung	Nicht unterstützt
Voicemail	Die Teilnehmer nutzen ihr lokales VoiceMail-System; es gibt keine zentrale VoiceMail für den gesamten Netzverbund.	Nicht unterstützt
Anwesenheitsstatus	Netzweit, innerhalb der OpenScape Business Vernetzung	Nicht unterstützt
Besetztanzeige	Netzweit, innerhalb der OpenScape Business Vernetzung	Nicht unterstützt
Internes Verzeichnis / Favoriten	Netzweit, innerhalb der OpenScape Business Vernetzung	Nicht unterstützt
Externes Verzeichnis	Lokal über den Import von CSV-Dateien	Nicht unterstützt
Suche in externen Verzeichnissen anderer Knoten	Nicht möglich	Nicht unterstützt
Externes Offline-Verzeichnis (LDAP)	über LDAP	Nicht unterstützt

Vernetzung von OpenScape Business

myAttendant	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
	Mit UC-Funktionalität über UC Booster Server, UC Booster Card oder OpenScape Business S	Nicht unterstützt
Sofortnachricht versenden	Netzweit, innerhalb der OpenScape Business Vernetzung	Nicht unterstützt
Voicemail	Die Teilnehmer nutzen ihr lokales VoiceMail-System; es gibt keine zentrale VoiceMail für den gesamten Netzverbund.	Nicht unterstützt
Anwesenheitsstatus	Netzweit, innerhalb der OpenScape Business Vernetzung	Nicht unterstützt
Besetztanzeige	Netzweit, innerhalb der OpenScape Business Vernetzung	Nicht unterstützt
Internes Verzeichnis / Favoriten	Netzweit, innerhalb der OpenScape Business Vernetzung	Nicht unterstützt
Externes Verzeichnis	Lokal über den Import von CSV-Dateien	Nicht unterstützt
Suche in externen Verzeichnissen anderer Knoten	Nicht möglich	Nicht unterstützt
Externes Offline-Verzeichnis (LDAP)	über LDAP	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	
Besetztanzeige	Netzweit	
Externes Verzeichnis	über LDAP	über LDAP
Zentraler Vermittlungsarbeitsplatz	Netzweit, innerhalb der OpenScape Business Vernetzung	

Company AutoAttendant (UC Suite)	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
Company AutoAttendant: Nachdem der AutoAttendant 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.	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	Nicht unterstützt

Company AutoAttendant (UCSmart)	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
Company AutoAttendant (UCSmart)	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.	Nicht unterstützt
VoiceMail (Aufnahme, Message Waiting Indication, Abfrage)	Die Teilnehmer nutzen ihr lokales VoiceMail-System; es gibt keine zentrale VoiceMail für den gesamten Netzverbund.	Nicht unterstützt
Anwesenheitsstatus	Netzweit	Nicht unterstützt
Besetztanzeige	Netzweit	Nicht unterstützt
Agentenstatus	Lokal	Nicht unterstützt
Internes Verzeichnis / Favoriten	Netzweit	Nicht unterstützt
Externes Verzeichnis	Lokal über den Import von CSV-Dateien	Nicht unterstützt
Suche in externen Verzeichnissen anderer Knoten	Nicht möglich	Nicht unterstützt
Externes Offline-Verzeichnis (LDAP)	Lokal	Nicht unterstützt
Übergabe eines Anrufs	Lokal	Nicht unterstützt

Vernetzung von OpenScape Business

myAgent	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
Kundeninformation	Lokal	Nicht unterstützt
Reporting	Lokal	Nicht unterstützt

Fremdapplikationen	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	Nicht unterstützt
Wahl einer öffentlichen Rufnummer im eigenen Knoten	Unterstützt	
Wahl einer öffentlichen Rufnummer in einem vernetzten Knoten	Netzweit, innerhalb der OpenScape Business Vernetzung	

Mobility	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
Desk Sharing	Innerhalb eines Knotens; Netzweit, innerhalb der OpenScape Business Vernetzung mit DLS	Nicht unterstützt
Mobility mit DTMF-Steuerung des Systems	Lokal (wird bei OpenScape Business S nicht unterstützt)	Lokal
myPortal to go (Web Edition), UC Suite	Netzweiter Anwesenheitsstatus und Verzeichnisse (jeder Knoten benötigt dafür entweder UC Booster Server, UC Booster Card, oder OpenScape Business S)	Nicht unterstützt

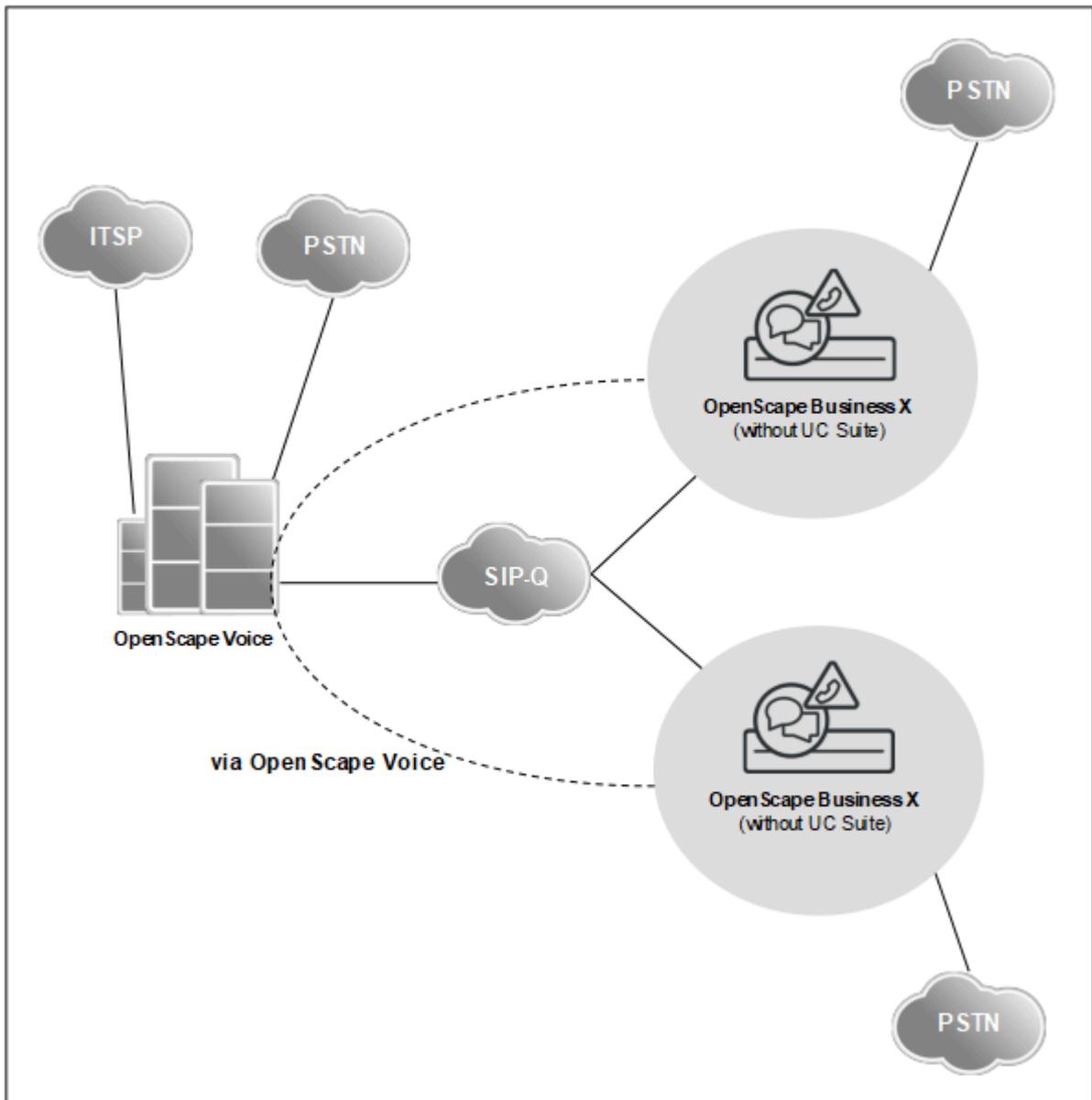
Mobility	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
myPortal to go (Web Edition), UC Smart	Lokal, nicht für UC Booster Server, UC Booster Card und OpenScape Business S	Nicht unterstützt
Sonstige Funktionalitäten	Geschlossene Nummerierung (Szenario 4a)	Offene Nummerierung (Szenario 4b)
Signaling- und Payload-Encryption (SPE)	Wird in OpenScape 4000 - OpenScape Business Vernetzungen unterstützt. Wird nicht unterstützt bei UC-Verbindungen und Konferenzen	Wird in OpenScape 4000 - OpenScape Business Vernetzungen unterstützt. Wird nicht unterstützt bei Konferenzen
DSS-Server	Netzweit, innerhalb der OpenScape Business Vernetzung	Nicht unterstützt
Anrufübernahme	Nicht unterstützt	Nicht unterstützt

20.6.7 Vernetzung von OpenScape Business X und OpenScape Voice

OpenScape Business X kann mit OpenScape Voice vernetzt werden.

Anmerkung: Ein Einrichteispiel 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.

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	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	
Lizenzierungsstruktur	Jeder Knoten einzeln, je OpenScape Business Knoten ist eine Netzlizenz erforderlich

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 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

Vernetzung von OpenScape Business

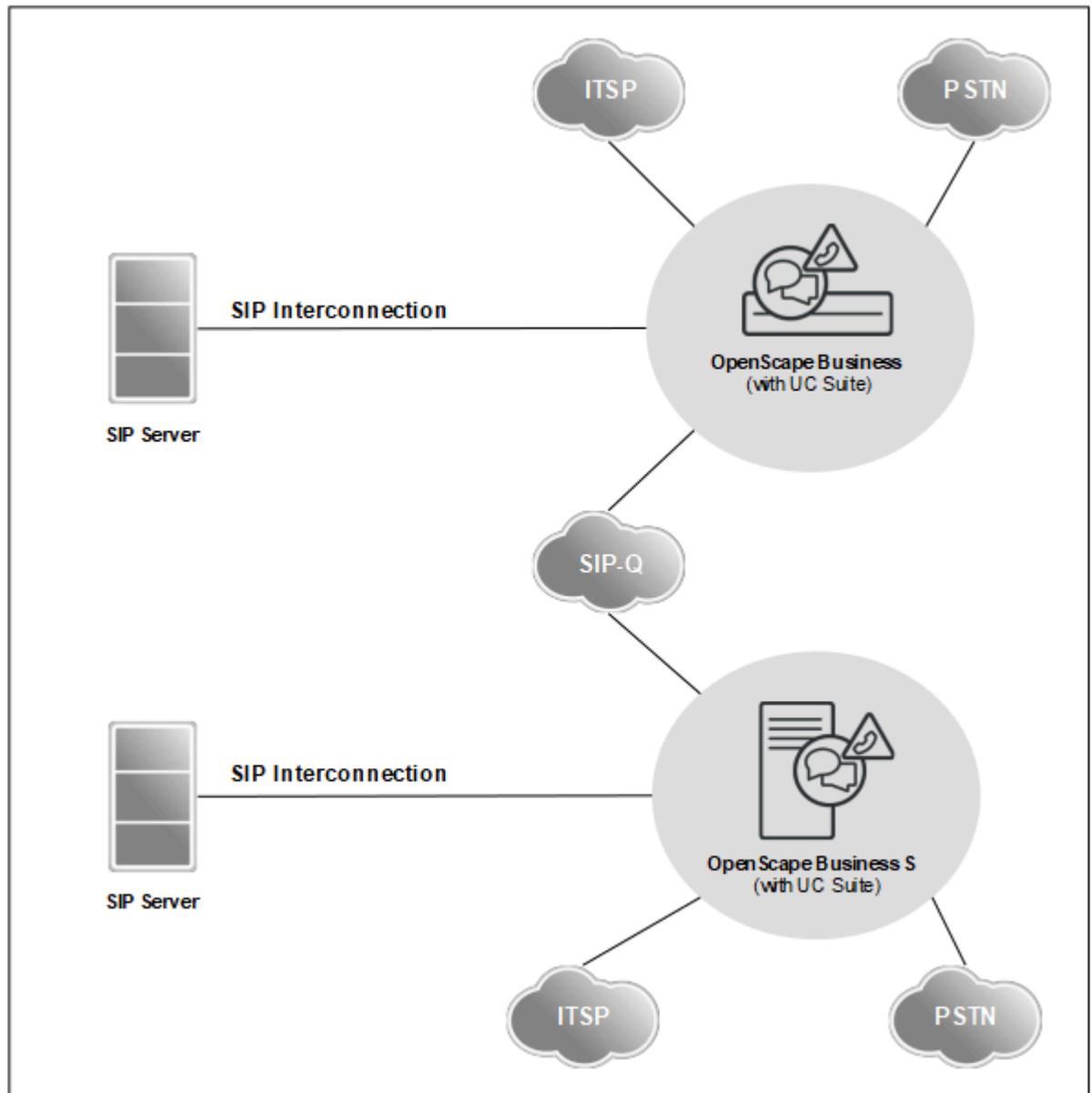
Verschlüsselungsprotokolls TLS erfolgen. SRTP (SDES) wird bei einer Vernetzung mit der OpenScape Voice V7R1 nicht unterstützt.

- 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.

20.6.8 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, OpenScape Voice oder andere zertifizierte SIP-Server nutzen zu können.

Voraussetzungen



- Es dürfen nur zertifizierte Applikationen angeschlossen werden wie z.B. OScaR.
- Ein externer SIP-Server kann über Native SIP- oder SIP-Q-Protokoll angeschlossen sein.
- Es stehen max. zwei SIP-Q-Richtungen zur Verfügung (eine wird für UC-Suite benötigt, falls vorhanden) und max. 10 Native SIP Richtungen (bis zu 8 Native SIP Richtungen können für ITSP verwendet werden).

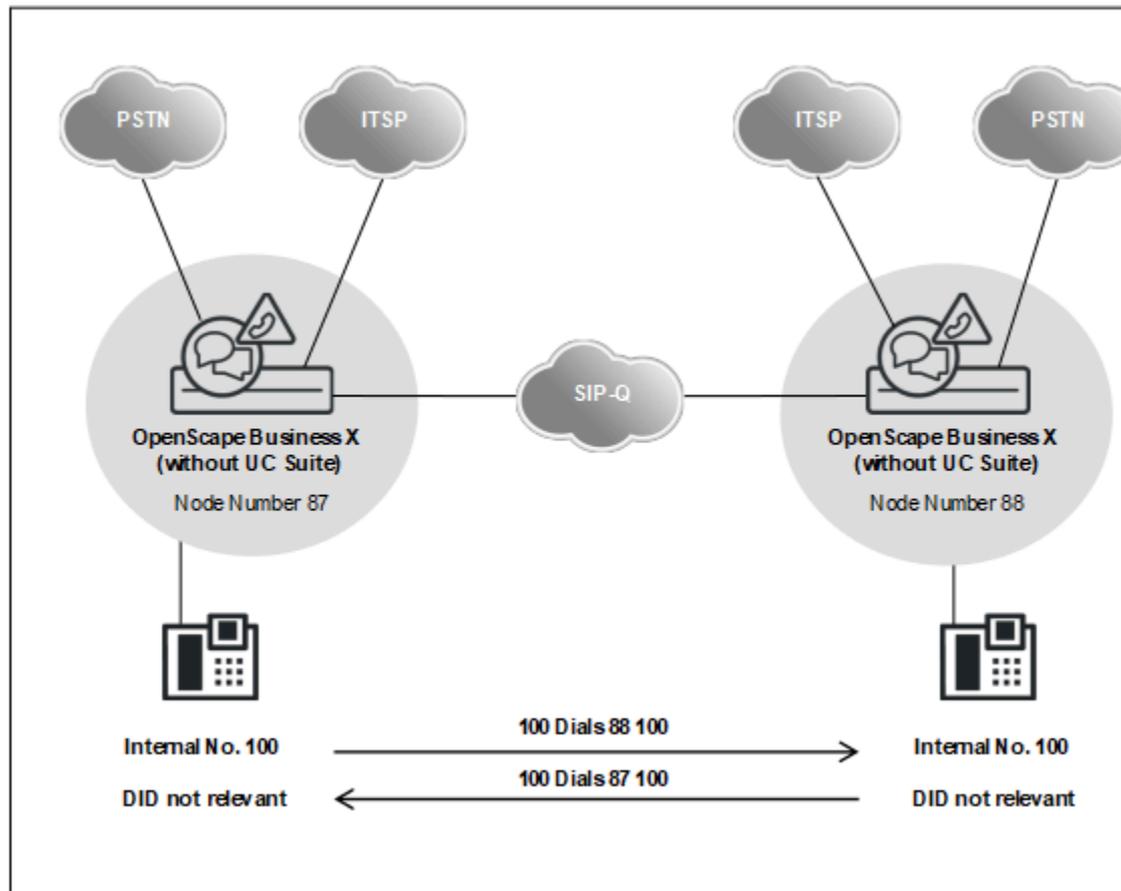
Weiterführende Information finden Sie im

- Experten-Wiki für Telefone, Kommunikationssysteme und UC:
<http://wiki.unify.com>

20.6.9 Offene Nummerierung in OpenScape Business X Netzwerken

Ein Netzverbund mit offener Nummerierung kann eingerichtet werden, wenn zwei (oder mehrere) Kommunikationssysteme vernetzt werden, bei denen die Nummerierung sich überschneidet (nicht eindeutig ist im Netzverbund).

Netzwerkdaten



- Netzweite Sprachvernetzung über OpenScape Business.
- UC-Leistungsmerkmale werden nicht unterstützt.
- 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 oder ITSP sind lokal an jedem Knoten möglich.

Anmerkung: Bei erweiterter netzweiter UC-Funktionalität ist eine Umstellung von offener auf verdeckte (geschlossene) Nummerierung erforderlich, um die internen Rufnummern anzupassen. Hierzu

muss die offene Nummerierung deaktiviert werden, um anschließend die Knotennummer zu löschen und als Präfix neu hinzuzufügen (beispielsweise als erweiterte Internrufnummer 87100 statt 100 und 88100 statt 100).

Unterschiede:

- Die Auswahl der Teilnehmer auf ihrem eigenen Knoten erfolgt über die erweiterte Internrufnummer.
 - Die interne und die DuWa-Rufnummer dürfen voneinander abweichen, die Durchwahlnummern dürfen jedoch nicht geändert werden.
-

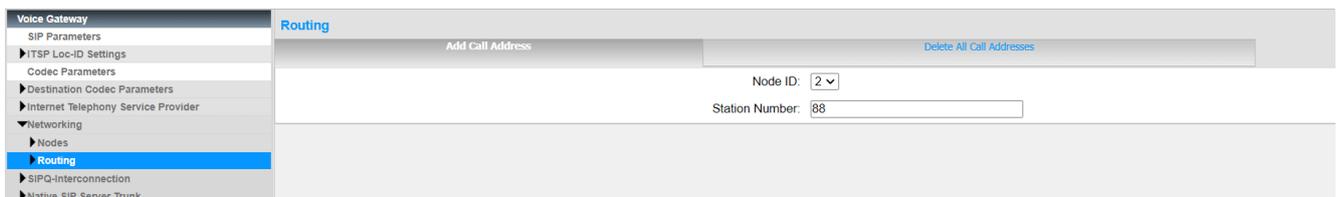
20.6.9.1 Wie Sie die offene Nummerierung konfigurieren

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 adressiert (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.

Vernetzung von OpenScape Business

Dial Plan	Name	Dialed digits	Routing Table	Acc. code	Classes of service	Emergency
56	Standard	861CZ	20	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
57	Standard	861C0-Z	20	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
58	Standard	861C1Z	20	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
59	Standard	861CNZ	20	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
60	Standard	861C00-Z	20	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
61	Standard	862CZ	22	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
62	Standard	862C0-Z	22	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
63	Standard	862C1Z	22	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
64	Standard	862CNZ	22	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
65	Standard	862C00-Z	22	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
66	Standard	863CZ	24	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
67	Standard	863C0-Z	24	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
68	Standard	863C1Z	24	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
69	Standard	863CNZ	24	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
70	Standard	863C00-Z	24	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
71	Standard	864CZ	26	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
72	Standard	864C0-Z	26	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
73	Standard	864C1Z	26	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
74	Standard	864CNZ	26	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
75	Standard	864C00-Z	26	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
76	Node 2 open Num	88	20	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

2) Anzeige der konfigurierten Route

Index	Dedicated Route	Route	Dial Rule	min. COS	Warning	Dedicated Gateway	GW Node ID
1	<input type="checkbox"/>	Networking	Node 2 open Nu	15	None	No	
2	<input type="checkbox"/>	None	None	15	None	No	
3	<input type="checkbox"/>	None	None	15	None	No	
4	<input type="checkbox"/>	None	None	15	None	No	
5	<input type="checkbox"/>	None	None	15	None	No	
6	<input type="checkbox"/>	None	None	15	None	No	
7	<input type="checkbox"/>	None	None	15	None	No	
8	<input type="checkbox"/>	None	None	15	None	No	
9	<input type="checkbox"/>	None	None	15	None	No	
10	<input type="checkbox"/>	None	None	15	None	No	
11	<input type="checkbox"/>	None	None	15	None	No	
12	<input type="checkbox"/>	None	None	15	None	No	
13	<input type="checkbox"/>	None	None	15	None	No	
14	<input type="checkbox"/>	None	None	15	None	No	
15	<input type="checkbox"/>	None	None	15	None	No	
16	<input type="checkbox"/>	None	None	15	None	No	

3) Den Namen der Route "Networking" und die dazugehörige Wahlregel "Node 2 open Num" eingeben.

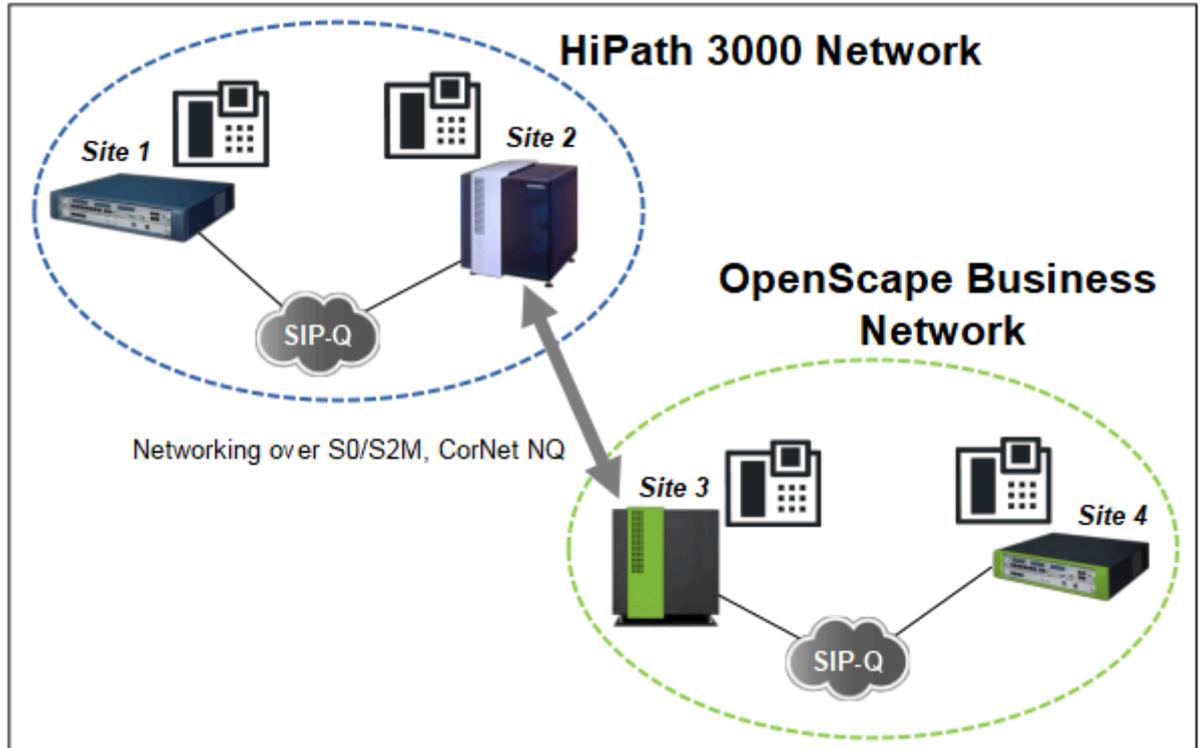
Rule Name	Dial rule format	Network access	Type
1 ISDN	A	Main network supplie	Unknown
2 SIP	A	Main network supplie	Unknown
3 SIP lokal	HE2A	Main network supplie	Unknown
4 MEB	E1A	Corporate Network	PABX number
5 IP-Network	A	Corporate Network	Unknown
6 Multi-Location	BA	Corporate Network	Unknown
7 Gateway call	E1A	Corporate Network	Unknown
8 COInternet	D0E4A	Main network supplie	Unknown
9 Add_cc_to_Canoni	D49E2A	Main network supplie	Country code
10 National_to_Cano	D49E3A	Main network supplie	Country code
11 Internat_to_Can	E3A	Main network supplie	Country code
12 SIP local_Canoni	HE2A	Main network supplie	Country code
13 networking_ext	D855019036891007	Main network supplie	Unknown
14 Node 2 open Num	E1A	Unknown	Unknown

20.6.10 Vernetzung über ISDN

OpenScape Business Systeme können sowohl untereinander als auch mit den Kommunikationssystemen HiPath 3000 und OpenScape 4000

über digitale Verbindungsleitungen vernetzt werden. Die Anschaltung kann sowohl über S_0 - 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 netzübergreifende Anruf über HiPath 3000/OpenScape Business wird über entsprechende TDM-Gateways geführt (S_0 oder S_{2M} 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

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 Feature-Sets der betroffenen Systeme. Daran kann abgelesen werden, inwieweit der theoretisch zu erwartende Leistungsumfang, d.h. der deckungsgleiche Anteil beider Feature-Sets 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.

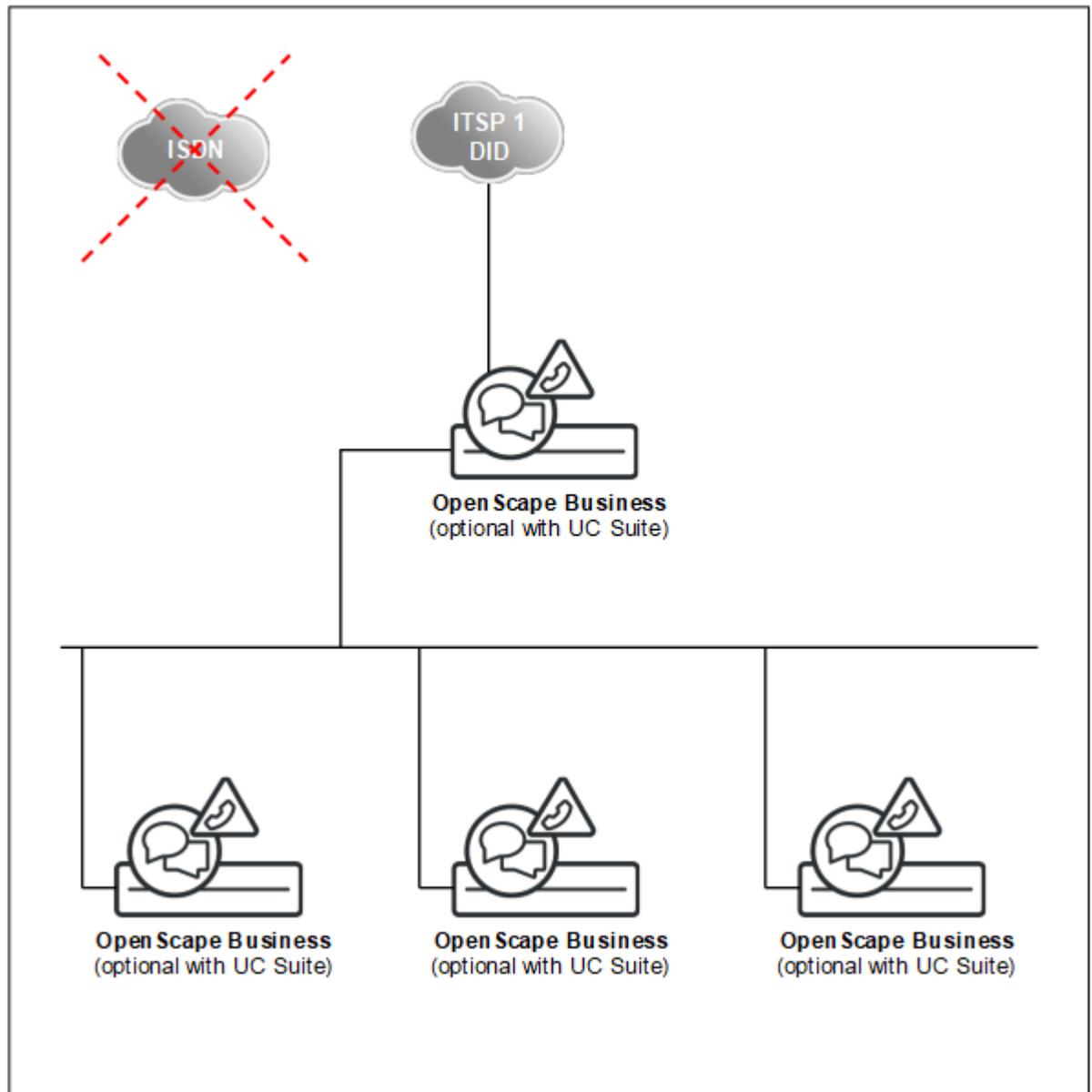
Anmerkung:

Die QSIG-Trunk-Gruppe sollte im OpenScape Business-System als PABX-Routentyp konfiguriert sein. Aus dem QSIG-Netz kommende Anrufe gelten daher als intern und folgen der internen CDL (Rufzielliste).

20.6.11 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

Vernetzung von OpenScape Business

Zentraler Abwurfplatz im Netzverbund (nicht für USA)

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-Amtrufnummern erfolgt in diesem Fall ausschließlich über die Durchwahl-Konfiguration des Teilnehmers (nicht über die Mapping-Tabelle, siehe ITSP-Konfiguration Kapitel 9.2 und siehe im Unify Experts Wiki im Internet).

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 Besetztssignal 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/Rufweitschaltung** 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 myAttendant (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.

20.8 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 am Master-Knoten des Netzverbundes oder eine OpenScape Business S als Master-Knoten. 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.

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 S₀-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 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 registriert.	Das System ist registriert.
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.	
	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.

Master

Slave

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.

Bei Aktivierung auf dem Master-Knoten werden die Slave-Knoten aufgefordert, Rufnummern und Namen des Systems vom Master zu aktualisieren.

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.

20.10 Survivability

Survivability ist ein Leistungsmerkmal innerhalb eines Netzwerks von OpenScope Business-Knoten. Ist ein OpenScope Business-Knoten ausgefallen oder aufgrund von Netzwerkfehlern nicht erreichbar, können sich die am OpenScope Business-Knoten angemeldeten Systemtelefone (HFA) stattdessen am anderen OpenScope Business-Knoten anmelden. Die Rufnummern der Systemtelefone bleiben nach der Neuansmeldung erhalten. Damit ist weiterhin die Basis-Telefonie gewährleistet, die Leistungsmerkmale der Applikationen wie z.B. myPortal, Voicemail und CTI werden vorübergehend ausgesetzt.

Callno	DID	First Name	Last Name	Display	Type	Clip/Lin	Active	Fax Callno
600	600	s600	netw_0	netw_0_s600	System Client	-	-	612
601	601	s601	netw_1	netw_1_s601	System Client	-	-	613
602	602	s602	netw_2	netw_2_s602	System Client	-	-	-
603	603	vosp_603	netw_3	netw_3_vosp_603	Deskshare User	-	-	-
604	604	vosp_604	netw_4	netw_4_vosp_604	Deskshare User	-	-	-
605	605	vosp_605	vosp_5	vosp_5_s605	System Client	-	-	-
606	606	vosp_606	netw_6	netw_6_vosp_606	Deskshare User	-	-	-
607	607	vosp_607	netw_7	netw_7_vosp_607	System Client	-	-	-
-	-	-	-	-	No Port	-	-	-
-	-	-	-	-	No Port	-	-	-
610	610	justle	WebRTC	WebRTC_justle	System Client	-	-	-
611	611	justle	Sip	Sip_justle	SIP Client	-	-	-
-	-	-	-	-	No Port	-	-	-
-	-	-	-	-	No Port	-	-	-
620	620	s620	netw_20	netw_20_s620	System Client	-	-	-
-	-	-	-	-	System Client	-	-	-
-	-	-	-	-	No Port	-	-	-
-	-	-	-	-	System Client	-	-	-
-	-	-	-	-	SIP Client	-	-	-
-	-	-	-	-	Deskshare User	-	-	-

Nachdem der ausgefallene OpenScope Business-Knoten wieder sicher erreichbar ist, wechseln die Systemtelefone automatisch zurück zum OpenScope Business-Knoten.

Das Umschalten auf das Standby-Gateway kann bis zu 30 Minuten dauern.

Wenn der OpenScope Business-Knoten 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. Die aktuellen Status der angemeldeten Telefone sind in **Experten-Modus > Diagnose-Protokolle** einsehbar.

Vernetzung von OpenScape Business

Die Survivability-Einstellungen werden an den Systemtelefonen konfiguriert. Wenn der OpenScape Business-Knoten ausfällt, versuchen die Telefone erst mehrmals, diesen wieder zu erreichen. Ein Time Out bzw. wie oft sich die Telefone wieder anzumelden versuchen, kann im Administrationsmenü der Telefone über "System Redundancy" konfiguriert werden. Die Standardeinstellung für das Timeout (Zeitüberschreitung) ist 30 Sekunden mit einem Wiederholungsversuch. Danach registrieren sich die Telefone am Standby-Gateway. Die automatische Rückanmeldung am OpenScape Business-Knoten ist ebenso auf den Systemtelefonen zu konfigurieren.

Die folgenden Voraussetzungen müssen für Survivability erfüllt sein:

- Für die Anzahl der am OpenScape Business-Knoten angeschlossenen Systemtelefone, die im Falle eines Netzknotenausfalls "gerettet" werden sollen, müssen am Standby-Gateway ausreichend freie IP-Ports vorhanden sein.
- Für diese freien Ports am Standby-Gateway müssen Teilnehmer ohne Namen und Rufnummer eingerichtet sein.

CallNo	DID	First Name	Last Name	Display	Type	Clip/Lin	Active	Fax CallNo	F
600	600	s600	netw_0	netw_0_s600	System Client	-	-	612	612
601	601	s601	netw_1	netw_1_s601	System Client	-	-	613	-
**602	-	s602	netw_2	netw_2_s602	System Client	-	-	-	-
603	603	voip_603	netw_3	netw_3_voip_603	Deskshare User	-	-	-	-
604	604	voip_604	netw_4	netw_4_voip_604	Deskshare User	-	-	-	-
605	605	s605	voip_5	voip_5_s605	System Client	-	-	-	-
606	606	voip_606	netw_6	netw_6_voip_606	Deskshare User	-	-	-	-
607	607	voip_607	netw_7	netw_7_voip_607	System Client	-	-	-	-
-	-	-	-	-	No Port	-	-	-	-
-	-	-	-	-	No Port	-	-	-	-
610	610	justle	WebRTC	WebRTC_justle	System Client	-	-	-	-
611	611	justle	Sip	Sip_justle	SIP Client	-	-	-	-
-	-	-	-	-	No Port	-	-	-	-
-	-	-	-	-	No Port	-	-	-	-
620	620	s620	netw_20	netw_20_s620	System Client	-	-	-	-
-	-	-	-	-	System Client	-	-	-	-
-	-	-	-	-	No Port	-	-	-	-
-	-	-	-	-	System Client	-	-	-	-
-	-	-	-	-	SIP Client	-	-	-	-
-	-	-	-	-	Deskshare User	-	-	-	-

- Die Teilnehmer müssen als Systemtelefone (System Clients) konfiguriert und eine Fallback-Benutzerlizenz haben. Wenn in der aktivierten Lizenzdatei keine Fallback-Lizenzen verfügbar sind, können stattdessen IP-Benutzerlizenzen verwendet werden. Die Teilnehmer können im Falle von Survivability ausschließlich Telefonie nutzen.

Anmerkung: Während der Ausfallzeit des Master-Knotens kommt es auf den HFA-Redundanz-Clients zu Rufnummernkonflikten, bis der Master-Knoten wieder betriebsbereit ist.

Anmerkung: Wenn dem System Fallback-Benutzerlizenzen zugewiesen sind, können IP-

Benutzerlizenzen im Falle eines Fehlerereignisses nicht verwendet werden.

The screenshot shows the 'License Management' section of the OpenScape Business interface. The 'IP User' tab is active, displaying a table of users and their licenses. The table has columns for 'Access', 'Call number', 'Display', and 'Remaining licenses'. The 'Remaining licenses' column is expanded to show a grid of license types and their counts. The interface includes a search bar, navigation icons, and a legend for license status.

Access	Call number	Display	Remaining licenses	1489	1489	1495	3234 *	1496	1497	18	187	500	150	1500
LAN 0-SYS-1	600	netw_0_s600		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>							
LAN 0-SYS-2	601	netw_1_s601		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>							
LAN 0-SYS-3	**602	netw_2_s602		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>							
LAN 0-SYS-6	605	voip_5_s605		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>					
LAN 0-SYS-8	607	netw_7_voip_607		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>					
LAN 0-SYS-9	610	WebRTC_justie		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN 0-SIP-3	611	Sip_justie		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN 0-SYS-12	620	netw_20_s620		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

20.11 Entfernung eines Knotens aus dem Netzverbund

Wenn ein Knoten aus dem Netzverbund entfernt werden soll, ist es wichtig das der Knoten in der Netzwerk-Konfiguration nicht mehr erreichbar ist. Sonst versucht dieser Knoten, sich selbständig wieder im Netzverbund anzumelden, und der Master-Knoten versucht, Daten zu synchronisieren.

Verfahren

Das Löschen eines Knotens erfolgt über den Wizard Vernetzung, wobei immer alle beteiligten Knoten entfernt werden müssen.

- Alle Strecken (Routing) zu den zu entfernenden Knoten unterbrechen.
- Administration des Netzverbundes
- Geben Sie für den betroffenen Slave-Knoten im Netzwerk-Assistenten des Slave-Knotens "Kein Netzwerk" ein.
- Entfernen Sie den Slave-Knoten im Netzwerk-Assistenten des Master-Knotens aus der Registrations-Liste.

Wird der Knoten nicht 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.

21 Anschaltungen

Anschaltungen sind externe Geräte (wie z.B. ein Ansagegerät oder eine Türsprechstelle mit Türöffner), die an die Schnittstellen des Kommunikationssystems angeschlossen 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).

Anmerkung: Stellen Sie vor der Benutzung von Ansagen bzw. Musik aus anderer Quelle sicher, dass Sie keine Copyright-Verletzung 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

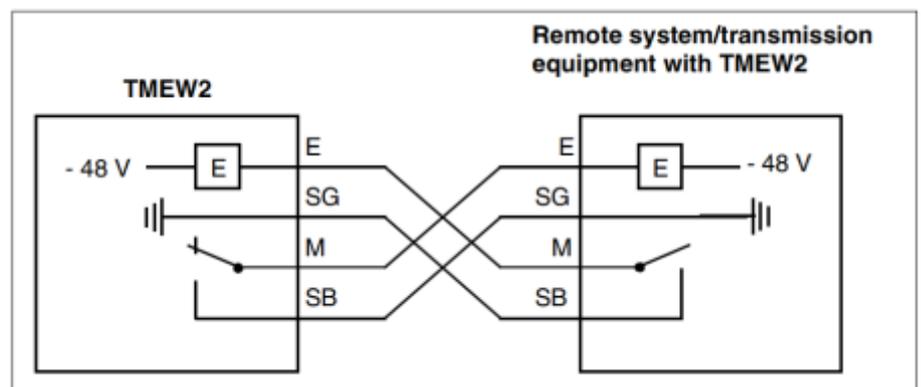
- OpenScape Business X3: STRBR-Optionsbaugruppe

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 Ansagegerätes Genius erfolgt mit dem Manager E über **Anlagensicht > Einstellungen > Anschaltungen > Ansage**.

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.

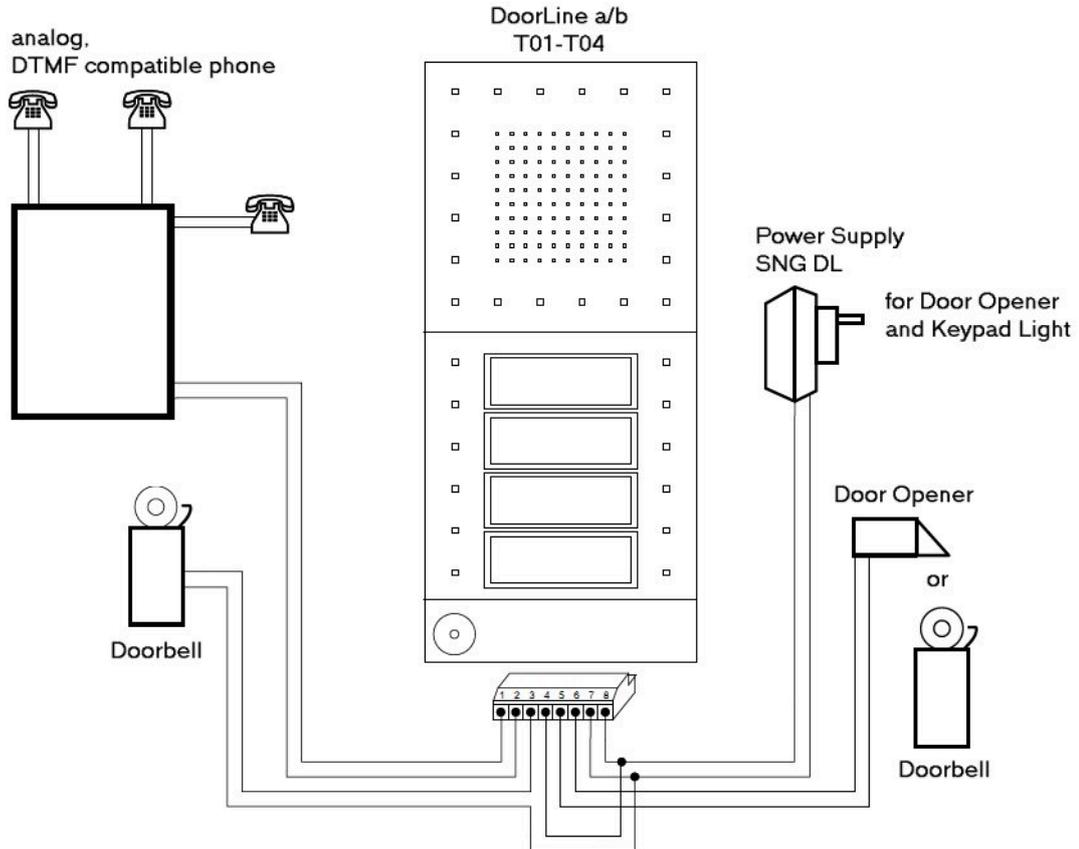
21.2.1 DoorLine a/b T01-T04

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

Anschaltungen

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.



Anmerkung: 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 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.

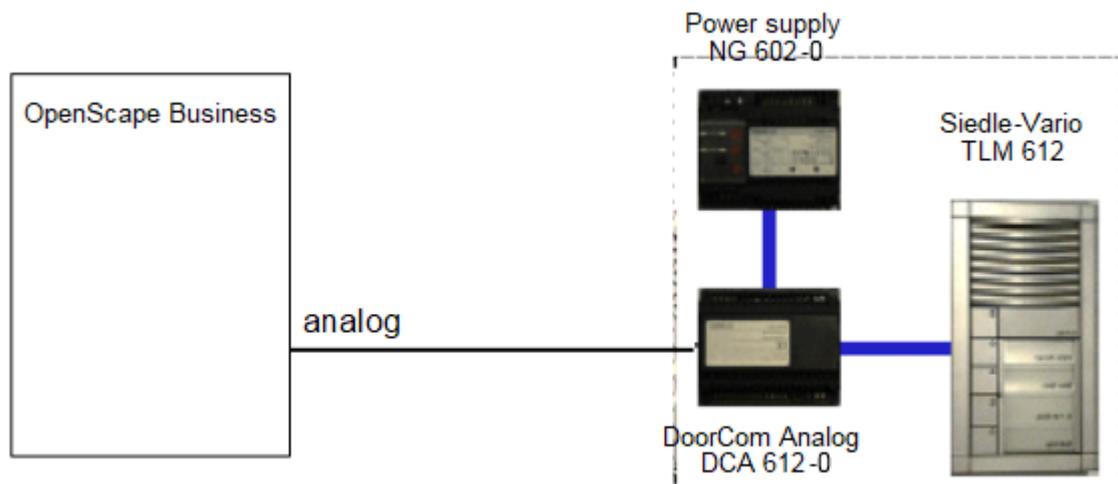
DoorCom Analog ist ausschließlich in Verbindung mit folgenden Komponenten funktionsfähig:

- 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.

Anmerkung: 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.

21.2.3 Türfreisprecheinrichtung mit Verstärker (TFE-S)

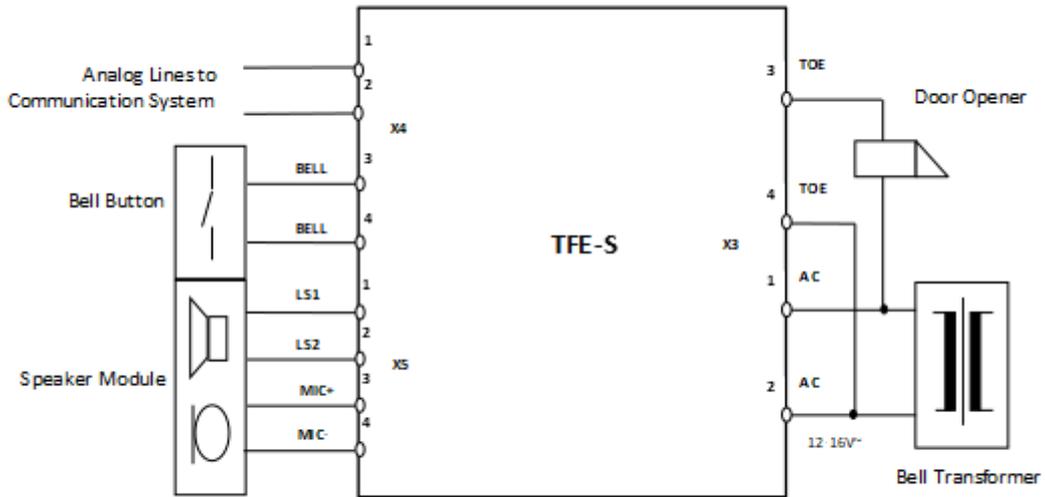
Das TFE-S Modul (S30122-K7696-T313) verbindet eine analoge Schnittstelle des Kommunikationssystems mit einer Türfreisprecheinrichtung, einem Türöffner und einem Klingeltaster. Die Steuerung erfolgt über das Kommunikationssystem.

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.

Anschaltungen



Technische Daten

Parameter	Wert
Stromversorgung	Klingeltrafo 12V - 16V AC, 50Hz
Stromaufnahme	Max. 150mA
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.

Tipp: Bei der Signalisierung eines Türrufs wird die Nachtschaltung nicht berücksichtigt.

Tipp: 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 Anruf-umleitung der Zielstelle folgen soll.

21.2.4 Lautsprecher

Lautsprecher können über Verstärker an das Kommunikationssystem angeschlossen werden.

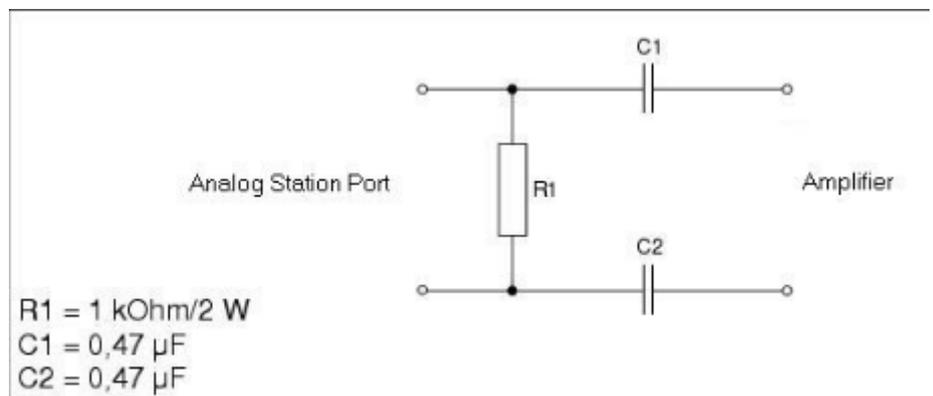
Für den Anschluss eines Verstärkers inkl. Lautsprecher bestehen folgende Möglichkeiten:

- **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**

Anschaltungen

Aktoren

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).

21.3 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:

Anmerkung: Die Kennzahlen für die Steuerung finden Sie im Kapitel "Experten-Modus".

- **Ohne Funktion**

Der Actor ist entweder nicht in Betrieb oder als zentraler Wecker eingetragen (unter "Einstellungen" - "Kommende Rufe" - "Rufziellisten").

- **Manuell ein und aus**

Der Actor 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: $30 \cdot 100\text{ms} = 3 \text{ sec}$.

- **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.

- **Wartemusik**

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. $600 \cdot 100\text{ms} = 60 \text{ sec}$). 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 deaktiviert. Der Aktor ist nicht getaktet. Dieser

Funktion muss ein bestimmter Teilnehmer zugeordnet werden. Wird als Schaltzeit ein Wert größer 0 eingegeben, wird eine Ausschaltverzögerung 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.

21.4 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:

Anmerkung: 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
 - 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
 - Kurzwahlssystem 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. Über einen an diese Schnittstelle angeschlossenen Anrufbeantworter kann eine Sprachansage angeschaltet werden, die dem angewählten Teilnehmer das Ansprechen des Sensors mitteilt. 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 Zusammenhang 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.

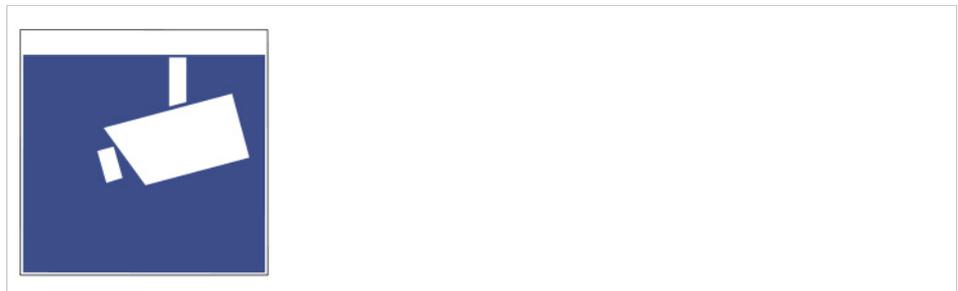
21.5.1 Rechtliche Rahmenbedingungen

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-Video-Stream.

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

Zeigt Details für alle aufgezeichneten Videodateien sowie Optionen für Wiedergabe, Download und Löschen an.

Status

Zeigt Informationen zur Hard- und Software des OpenStage Gate View Systems.

Administration

- **Wartung**

Ermöglicht das Löschen von Software- und Benutzer-Daten.

- **Konfiguration der Aufnahme**

Ermöglicht die Konfiguration des Aufnahmegerätes und der Aufnahmeart.

- **Türöffner**

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-Konfiguration 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.

21.5.6 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.

21.5.7 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 Mediatix/AP1120-Gerätes zum Anschluss 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.

21.5.8 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 Benutzernamen 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.

21.5.9 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 herunterladen.

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.

Bitte beachten Sie, dass Gate View nicht garantiert, dass alle Kameras als "Andere" unterstützt werden. Nur einige Kameras sind funktionsfähig, während einige andere überhaupt nicht funktionieren.

22 Application Connectivity

Application Connectivity unterstützt das System z. B. mit CSTA, TAPI sowie mit Application Launcher.

22.1 CSTA

Die CSTA-Schnittstelle ermöglicht die Anbindung von hochperformanten CTI-, Contact Center- und Unified Communications-Applikationen etc. an OpenScape Business.

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
- Unterstützung des CSTA XML Protokolls für zertifizierte Applikationen
- Breite Palette von unterstützten Systemtelefonen
- Netzweites Monitoring und Steuerung aller Ressourcen
- Multiplexing für Monitorpunkte

Unterstützte Geräte

CSTA unterstützt zusätzlich zu den vom System unterstützten Telefonen folgende Geräte:

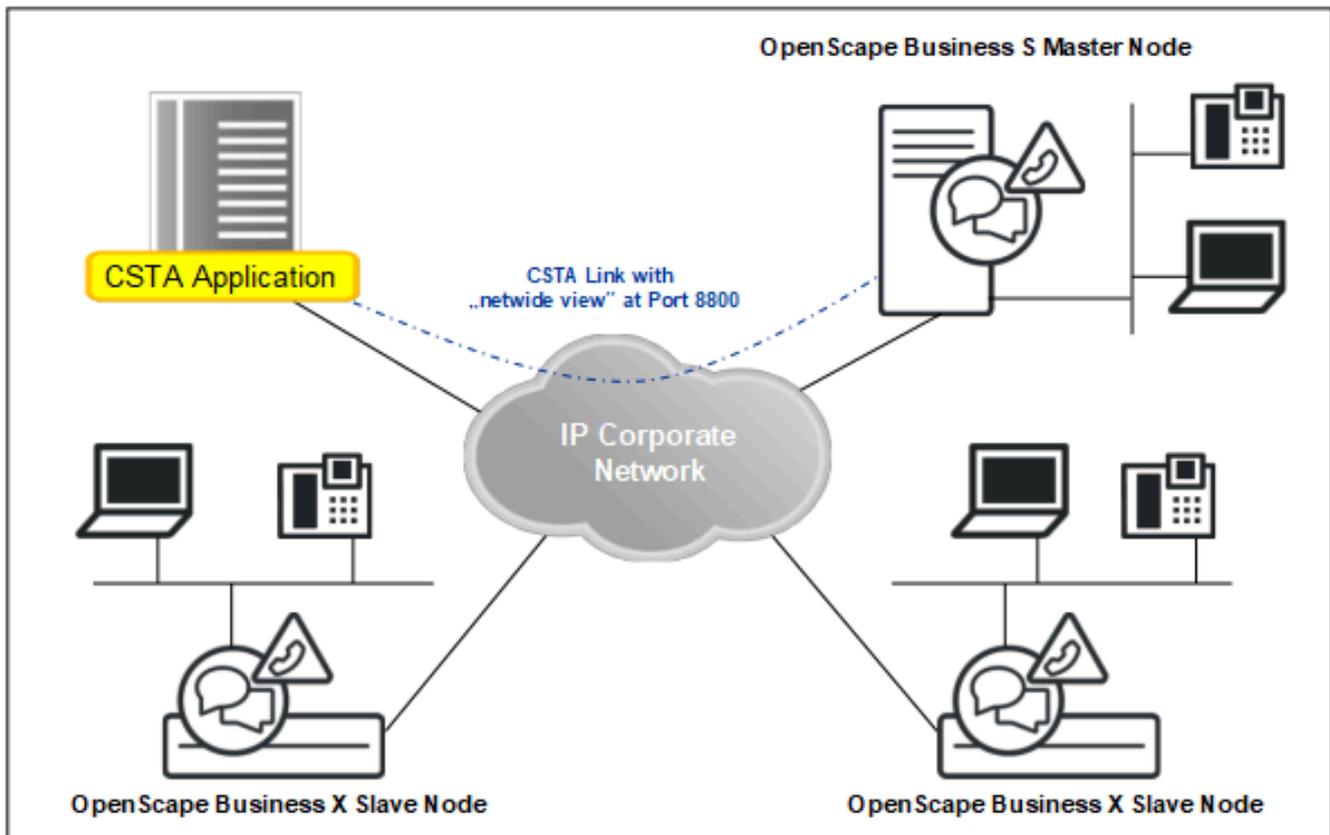
- ITSP
ermöglicht z.B. die Nutzung von Call Center-Applikationen mit SIP-Amtsleitungen
- ISDN
- Amt analog

Application Connectivity

- Virtuelle Teilnehmer
- UCD-Gruppen
- MULAPs

Anmerkung: 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	Verwendung
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.

Anmerkung: Ein CSTA-Link stellt den TDS-Dienst nur für lokale Geräte zur Verfügung. Kunden benötigen einen CSTA-Link zu jedem Knoten, der den TDS-Dienst bereitstellen soll.

Generell können CSTA-Anwendungen über CSP, über LAS (eine Systemkomponente) oder über PCC (eine LDH-Komponente) an ein OpenScape Business System angeschlossen werden.

Anmerkung: Wenn eine Anwendung über CSP angeschlossen wird, müssen auch die Anmeldeinformationen gegen CSP eingerichtet werden.

Insbesondere:

- Die (externen) Anwendungen UC Suite, OSCC, TAPI 170 und 3rd Party werden über CSP angeschlossen

Die Anbindung von (externen) CSTA-Anwendungen von Drittanbietern, die Trunk-Informationen benötigen, kann nur im UC Suite-Modus oder durch Abfrage der Trunk-Überwachungspunkte selbst über CSTA in deren eigener Anwendung erfolgen.

- Circuit und NGTC werden über PCC angeschlossen
- UC Smart wird über LAS angeschlossen

Plus-Produkte

Folgende Flags sind im System stets aktiviert:

- Vorwahl stets mit Rufnummer übertragen
- Erweitertes CSTA-CAUSE Handling
- CSTA CSP Signalisierung
- MULAP Monitoring

Zugehörige Konzepte

[Unterstützte Telefone](#) auf Seite 69

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 wesentlichen 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 unterliegen 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 Betriebsmodi 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.

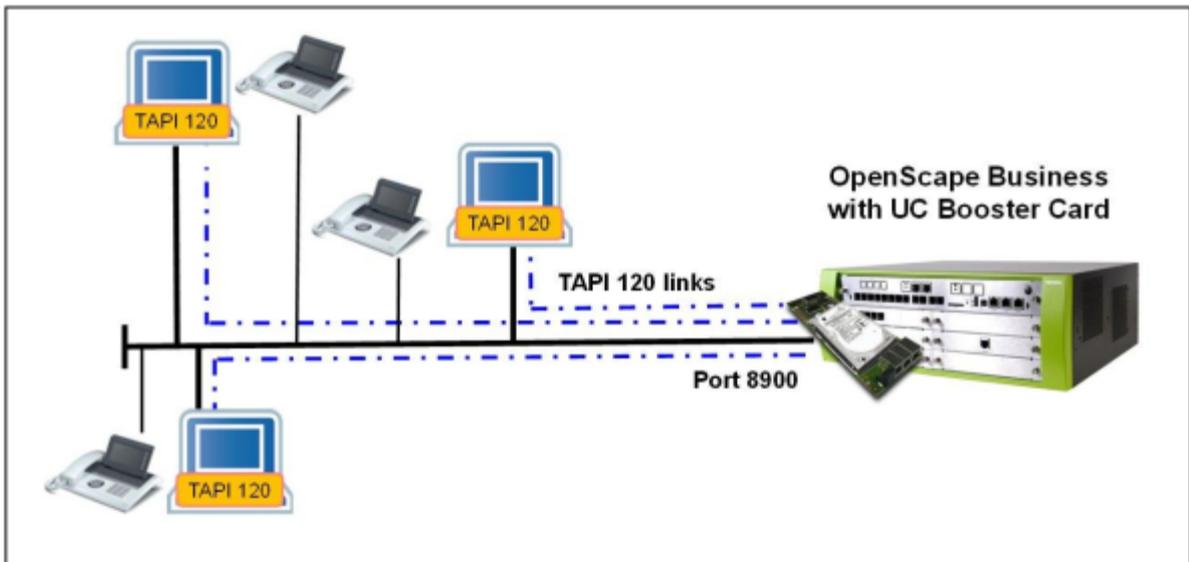


Abbildung 9: TAPI 120 im CSTA Modus mit OpenScape Business X5R und UC Booster Card

- **TAPI 120 UC Smart Modus**

Alle TAPI 120 Client PCs werden über LAN und WebServer Interface an das Mainboard von OpenScape Business angeschlossen. OpenScape Business multiplext intern alle TAPI 120 Verbindungen.

TAPI 120 im CSTA Modus unterstützt OpenScape Business X1/X3/X5/X8.

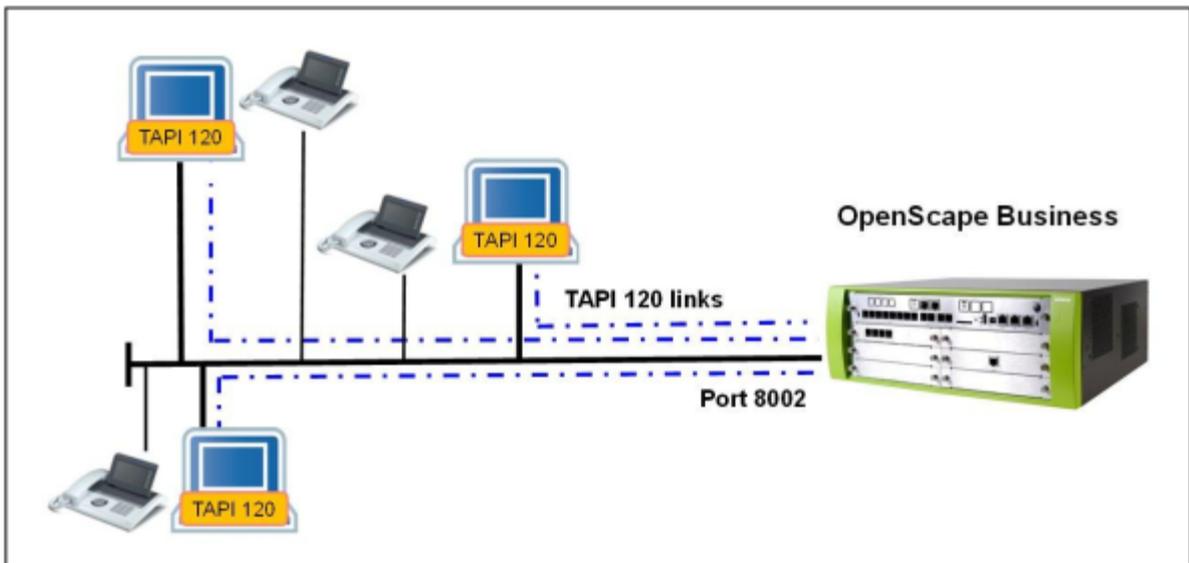


Abbildung 10: TAPI 120 im UC Smart Modus mit OpenScape Business X5R

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
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	-

Leistungsmerkmal	TAPI 120 CSTA	TAPI 120 UC Smart
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/ Lautsprecher/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 angeschlossen 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 aktuellen 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 im OpenScape Business System verwaltet und können für beide Modi von TAPI 120 verwendet werden. Bei Verwendung des Leistungsmerkmals MULAP ist für jeden Teilnehmer innerhalb der MULAP eine TAPI-Lizenz erforderlich.

Anmerkung: Bei TAPI 120 im UC Smart Modus sind keine UC User-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 Geräte

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 eingegeben werden. Diese IP-Adresse wird im WBM unter **Applikationsauswahl** angezeigt.

Zugehörige Tasks

[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 Übergeben
 - 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 OpenScope Business TAPI 170 konfiguriert sind. Die TAPI 170 Software wird über LAN an die CSTA Schnittstelle von OpenScope Business angebunden. Für diese Anschaltung wird ein CSTA Link von OpenScope Business sowie je eine TAPI-Lizenz für jeden eingerichteten TAPI-Teilnehmer benötigt.

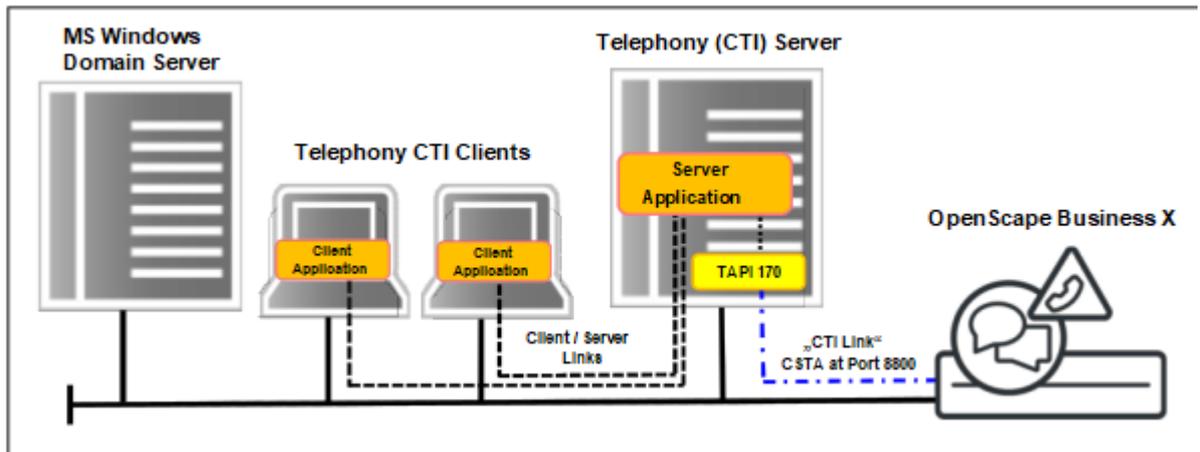


Abbildung 11: Serverbasierte TAPI-Anwendung über TAPI 170 an OpenScope Business

- **Anschaltung clientbasierter TAPI-Anwendungen an OpenScope Business über TAPI 170 mit "Remote TAPI" Funktion**

In diesem Szenario wird die OpenScope Business TAPI 170 Software auf einem Server im Netzwerk installiert. Auf den Client PCs mit den TAPI-Anwendungen wird sogenannte "Remote TAPI" Funktion freigeschaltet, über die die TAPI-Anwendung 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 OpenScope Business angebunden. Für diese Anschaltung wird ein CSTA Link von OpenScope Business sowie je eine TAPI-Lizenz für jeden eingerichteten TAPI-Teilnehmer benötigt.

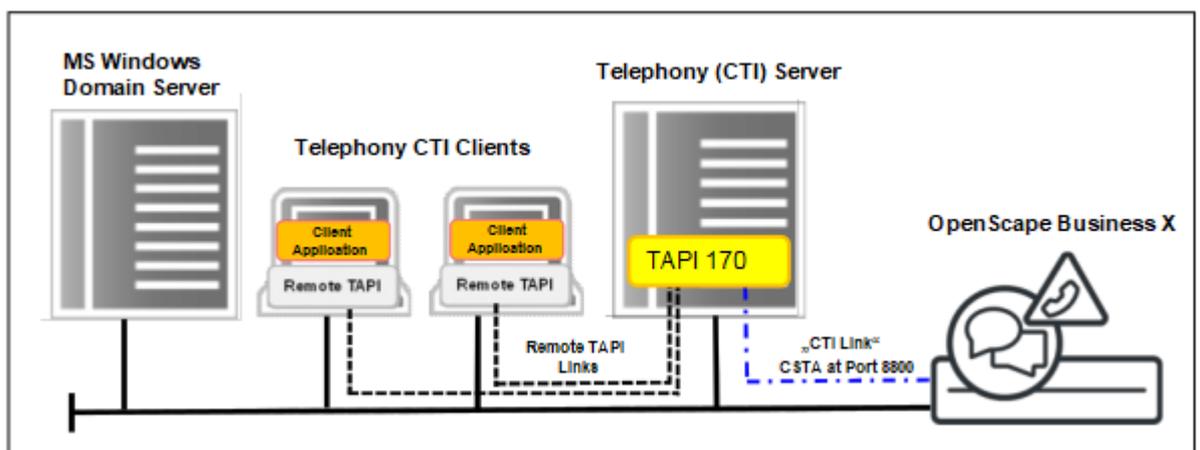


Abbildung 12: Clientbasierte TAPI-Anwendung über "Remote TAPI" an OpenScope Business

- **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.

Anmerkung: 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.

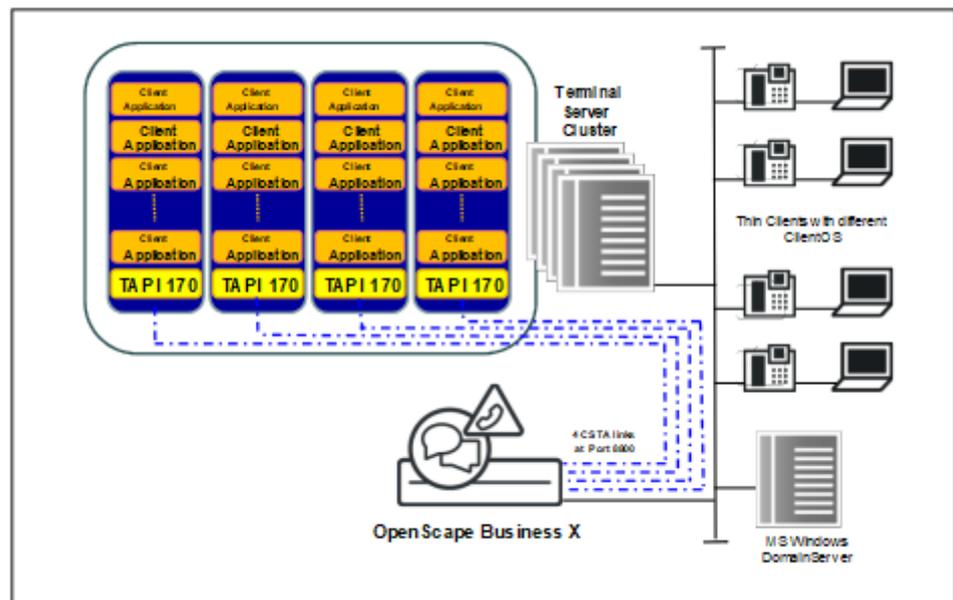


Abbildung 13: Client basierte TAPI Applikation auf Terminal-Server an OpenScape Business

- **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 angeschlossen 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.

Anmerkung: 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.

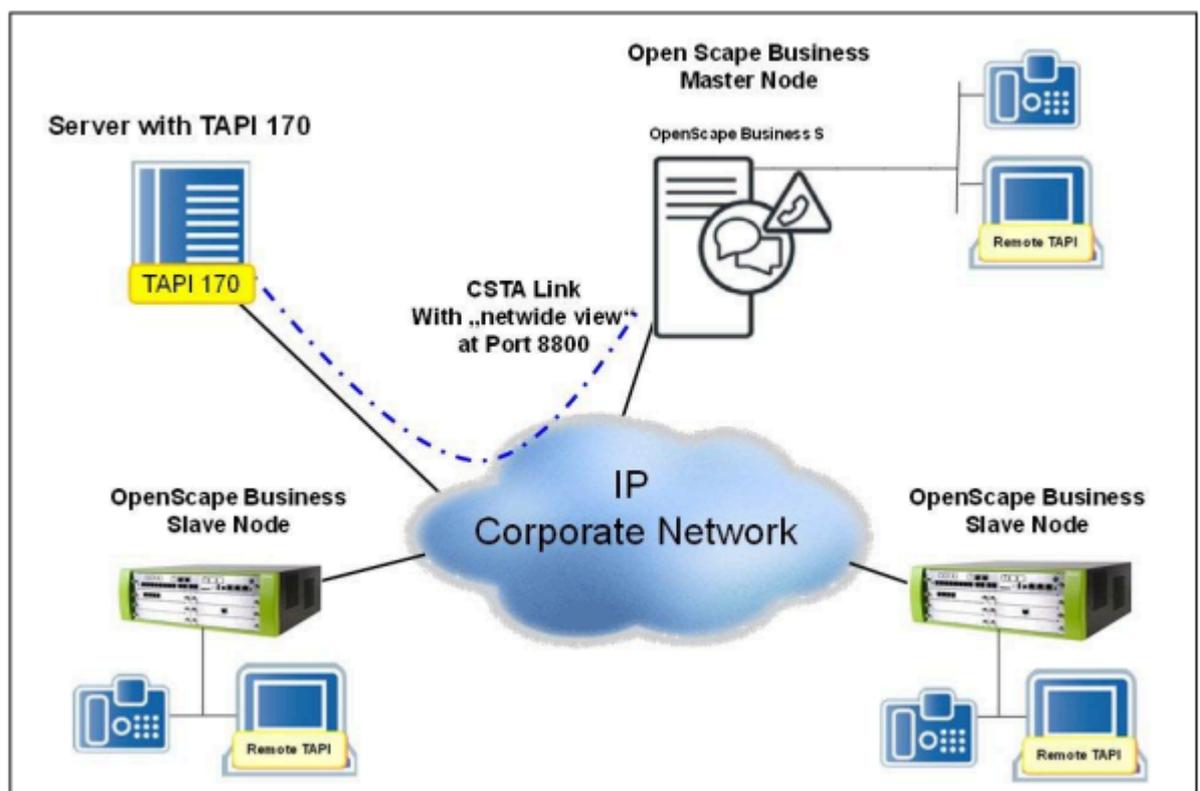


Abbildung 14: Anschaltung von TAPI 170 an vernetzte OpenScape Business Systeme

Ausbaugrenzen

Die maximal Anzahl von TAPI 170 Client PCs, die an OpenScape Business angeschlossen 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 aktuellen 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 Geräte

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
 - Verzeichnisse
 - Journal der Teilnehmer
 - Anwesenheitsstatus der Teilnehmer

Anmerkung: Abhängig vom verwendeten (Web Services Interface) WSI-Clienttyp muss das Flag Assoziierte Dienste aktiviert werden, um die Ausführung einiger WSI-Befehle zu ermöglichen.

Web Server WebSessions

Die Anzahl der verfügbaren Web Server Sessions gilt für alle entsprechenden Anwendungen gemeinsam, wie z.B. myPortal to go (Web Edition), 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 Datenquellen in Verzeichnisse des Systems und andererseits die Bereitstellung von Verzeichnissen an Clients, Kommunikationsgeräte und Anwendungen.

OpenScape Office 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 interne Datenquellen stehen in Open Directory Service standardmäßig zur Verfügung:

- Externes Verzeichnis
- Internes Verzeichnis
- Zentrale Kurzwahlnummern

Für diese internen Datenquellen sind die Feldnamen dem Datenschema von Open Directory Service fest zugeordnet.

Diese internen Datenquellen können nicht gelöscht oder geändert werden.

Externe Datenquellen

Als Administrator können Sie Kontaktdaten aus folgenden Arten von Datenbanken als Datenquellen für Lesezugriff via ODBC einbinden:

- Datenquellen mit eingebauten Treibern (Microsoft SQL Server, PostgreSQL, Sybase, SQL Server).
- Datenquellen mit eingebauten Treibern benötigen einen installierten und konfigurierten ODBC Bridge Server auf dem ODS-Client (downloadbar über das WBM unter **Service-Center > Software**).

Anmerkung: Für eine erfolgreiche Verbindung ist es notwendig, im Feld **Beschreibung** einen Wert zu definieren (der Wert kann sich vom Namen der Datenquelle unterscheiden, das Feld darf aber nicht leer sein). Im Falle einer ODBC-Bridge-Datenquelle für Access-, Firebird-, Excel- und Oracle fügen Sie in das Feld **Beschreibung** jeweils den Namen der Datenquelle ein, also „access“, „firebird“, „excel“, „oracle“.

Maximale Anzahl unterschiedlicher Arten von Datenbanken: 3

Maximale Anzahl externer Datenquellen: 4

Sorgen Sie dafür, dass Open Directory Service berechtigt ist, auf die externe Datenquelle zuzugreifen. Kontaktieren Sie hierfür vorab den zuständigen Datenbankadministrator. Unter Umständen muss in der externen Datenquelle 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 konfigurieren.

Eine Spalte, die als ID dient, muss eindeutige Werte enthalten; sie darf weder leer sein noch den Wert Null 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.
- Die Zwischenraum-Leerzeichen (mindestens in den letzten 4-5 Ziffern) werden vom ODS für Telefondaten 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 der Art 1:1 oder n:1 entsprechen, 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 potenziellen Sicherheitsrisiken werden nicht ausgeführt, z.B.:

- Ändern von Daten
- Anhalten des SQL-Servers
- Ausführen von Programmen durch den SQL-Server
- Ändern von Benutzerrechten

Benutzerdefinierte SQL-Abfragen mit folgenden SQL-Befehlen 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-Ausgabebezuordnungen

Eine LDAP-Ausgabebezuordnung 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-Ausgabebezuordnung **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 zudem weitere LDAP-Ausgabebezuordnungen konfigurieren.

Über den Parameter `dc` im LDAP-Login können LDAP-Clients auf eine bestimmte LDAP-Ausgabebezuordnung 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 das Wählen über den Desktop 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 Ortsvorwahl usw. aus dem System automatisch eintragen lassen. Falls sich die externe Datenquelle an einem anderen Standort als das System befindet, müssen Sie diese Werte eventuell anpassen.

Status der Datenquellen

Die Statusanzeige unter **OpenDirectory > Datenquellen** hat folgende Bedeutung:

Farbe	Status
Grün	aktiviert
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
- Systemverzeichnis
- OpenStage-Telefone mit lokaler LDAP-Unterstützung
- DECT-IP-Telefone (über LDAP)
- SIP-Telefone (über LDAP)
- Anwendungen, z.B. CRM-Suites wie Microsoft Dynamics CRM (über CSV-Export für LDAP, ODBC oder OpenLDAP)

Open Directory Service kann anhand der Suchergebnisse erkennen, aus welcher Datenquelle ein Treffer stammt.

Zugehörige Konzepte

[Voraussetzungen für Application Launcher](#) auf Seite 681

22.5 Active Directory Integration Service

Active Directory ist ein Microsoft-Verzeichnisdienst für Domänennetzwerke. Mit dem angebotenen Active Directory Integration Service kann OpenScape Business die Active Directory Datenbank lesen und Benutzer mit seiner eigenen Datenbank synchronisieren, um die Benutzeradministration zu erleichtern und Konfigurationsaufwand zu verringern.

Voraussetzungen

Damit die Synchronisierung des Active Directory Integration Service stattfinden kann, müssen die folgenden Voraussetzungen erfüllt sein:

- Active Directory Microsoft Server ist vom Kunden bereitgestellt.
- Active Directory wird als zentraler Konfigurationspunkt für Mitarbeiterdaten, und insbesondere Benutzerdaten, verwendet.

Folgende Felder werden zwischen Active Directory und OpenScape Business zugeordnet:

- Vorname
- Nachname
- Anzeigename
- Nur dieses Active Directory wird zum Hinzufügen, Ändern oder Löschen von Daten von Mitarbeitern verwendet.
- Es wird erwartet, dass alle Active Directory-Änderungen automatisch auch auf dem Kommunikationssystem gelten.

Synchronisierung

Die eindeutige ID der OpenScape Business Teilnehmer, die für die Synchronisierung verwendet wird, ist die Durchwahlnummer. Diese Nummer wird mit dem Feld telephoneNumber das AD (Active Directory) synchronisiert.

Jede Änderung, die im Active Directory des Unternehmens erfolgt, wird umgehend mit OpenScape Business synchronisiert. Das bedeutet, dass jeder neue Teilnehmer, der zum AD hinzugefügt wird, auch zu OpenScape Business hinzugefügt wird, und dem Teilnehmer eine IP-Teilnehmerlizenz zugewiesen wird.

Alle Änderungen, die im AD an bereits synchronisierten Teilnehmern erfolgen, spiegeln sich umgehend bei OpenScape Business Teilnehmern wider.

Wenn ein synchronisierter Teilnehmer aus dem AD gelöscht wird, werden firstName, sn und displayName des Teilnehmers auch aus OpenScape Business gelöscht und die IP-Teilnehmerlizenz wird freigegeben. Die Durchwahlnummer und die interne Rufnummer werden jedoch nicht aus OpenScape Business und bleiben für die Zuweisung zu einem anderen Teilnehmer verfügbar.

Anmerkung: Der Zugriff auf den Active Directory Service ist schreibgeschützt. Dies bedeutet, dass die Synchronisierung der Benutzerdaten nur von Active Directory zu OpenScape Business erfolgt. Änderungen in den OpenScape Business Teilnehmerinformationen werden nicht wieder mit Active Directory synchronisiert und bei der nächsten Synchronisierung mit Active Directory Daten überschrieben.

Feldzuordnung

Sie können die Zuordnung der Feldnamen zum Datenschema des Active Directory Service anpassen. Auf diese Weise können Sie kontrollieren, wie Felder in OpenScape Business von Active Directory Daten aktualisiert werden.

Die Standardzuordnung der Felder ist in der folgenden Tabelle angegeben:

OpenScape Business Feld	Active Directory Feld
Vorname	Vorname
Nachname	sn

OpenScape Business Feld	Active Directory Feld
Anzeigename	displayName
Durchwahl	telephoneNumber

Normalisierung von Durchwahlnummern

Die Gateway-Standortdaten des OpenScape Business Systems werden verwendet, um die Durchwahlnummer eines Teilnehmers in das kanonische Nummernformat umzuwandeln.

Das Format von telephoneNumber in Active Directory muss ebenfalls im kanonischen Format sein, damit eine automatische Synchronisierung möglich ist.

22.6 Application Launcher

Application Launcher ist eine Java-basierte Windows-Anwendung zur anrufbezogenen Steuerung von Anwendungen, die auf den Client-PCs von UC Suite-Benutzern und myAgent-Benutzern ausgeführt werden. 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.

Die Installation erfordert lokale Administratorrechte auf dem Client-PC, automatische Updates jedoch nicht.

Betriebssystem

Application Launcher kann in Verbindung mit folgenden Betriebssystemen verwendet werden:

- Microsoft Windows 10 / 8.1 / 8 / 7 (jeweils als 32 Bit oder 64 Bit möglich)
- Microsoft Windows Vista (32 Bit)

Tipp: Das verwendete Betriebssystem benötigt stets den aktuellen Stand aller verfügbaren Updates (Service Packs und Patches).

Windows Update

Die PCs benötigen stets den aktuellen Stand aller verfügbaren Updates einschließlich Service Packs.

Zusätzliche Software

Auf einem PC muss Oracle Java Version 8 oder höher bzw. OpenJDK 8 installiert sein (siehe **Service-Center** > **Software**)

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.

Zugehörige Konzepte

[Konfiguration von myPortal to go und Mobility Entry](#) auf Seite 541
[Open Directory Service](#) auf Seite 675

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.

22.7 Circuit

OpenScape Business Benutzer können Anrufe über den Circuit-Client tätigen. Diese Funktionalität ist sowohl vom Circuit-Client aus als auch über das Gerät verfügbar. Hierzu müssen Sie die Circuit-Verbindung zu OpenScape Business konfigurieren und Circuit-Benutzer hinzufügen.

Die verfügbare Circuit-Funktionalität beinhaltet:

- Anrufe durchführen/annehmen
- Anrufe löschen/abweisen
- Anrufe halten/wiederaufnehmen
- Automatische/Manuelle Gesprächsübergabe
- Anruf weiterschalten/verschieben
- Konferenzruf
- Belegt in einer Gesprächsinformation
- DTMF-Unterstützung
- Rückfrageanruf
- Anruf tauschen
- Anrufumleitung
- Interworking deaktivieren
- Anklopfen
- Alternative Nummer
- Anruf-Routing
- Circuit-Teams

Anmerkung: Um den Status eines OpenScape Business-Benutzers bei der Änderung von Circuit zu aktualisieren, muss das Flag **OpenScape Business erweiterte Telefoniefunktionen** unter **Circuit Labs** aktiviert werden.

Anmerkung: Für die Anklopffunktion muss die Einstellung zum Ablehnen des Anklopfens für alle MULAP-Mitglieder gleich sein, weil andernfalls Client-GUI, Anrufjournal usw. irreführende Informationen haben könnten.

22.8 myPortal for Teams im Überblick

Das myPortal for Teams-Plugin wird verwendet, um die Microsoft Teams-Anwendung mit OpenScape Business zu integrieren.

myPortal for Teams erfordert ein neues OpenScape Business V3-Mainboard oder OpenScape Business S System und wird ab Software-Release V3R1 FR2 unterstützt.

Mit myPortal for Teams sind Sie in der Lage:

- Ihre Anrufliste zu filtern und zu verwalten.
- Kontakte anzuzeigen und zu suchen.

- Kontakte in Favoritengruppen zu organisieren.
- E-Mail-Kontakte.
- Ein zugeordnetes Telefon auszuwählen (für MULAP-Benutzer).
- Einen Anruf zu starten.
- Einen Anruf anzunehmen, abzulehnen oder weiterzuschalten.
- Einen Anruf zu halten.
- Einen Anruf zu übergeben.
- Einen Rückfrageanruf zu tätigen.
- Zwischen Anrufen zu wechseln.
- Ein Gespräch zu übergeben.

Anmerkung: Die Suche nach Kontakten in externen Verzeichnissen, wie z. B. LDAP, ist nicht verfügbar.

Anmerkung: Die VoIP-Funktionalität wird für myPortal for Teams nicht unterstützt.

22.9 Unify Phone

OpenScape Business Benutzer können Anrufe über den Unify Phone-Client tätigen. Diese Funktionalität ist sowohl vom Unify Phone-Client aus als auch über das Gerät verfügbar. Hierzu müssen Sie die Unify Phone-Verbindung zu OpenScape Business konfigurieren und Unify Phone-Benutzer hinzufügen.

Die verfügbare Unify Phone-Funktionalität beinhaltet:

- Anrufe durchführen/annehmen
- Anrufe löschen/abweisen
- Anrufe halten/wiederaufnehmen
- Anruf weiterschalten/verschieben
- DTMF-Unterstützung
- Anruf tauschen
- Anrufumleitung
- Alternative Nummer
- Anruf-Routing

Neben den oben genannten Funktionen werden keine weiteren Funktionen, insbesondere keine Funktionscodes, veröffentlicht.

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).

Zugehörige Konzepte

[Projektkennzahlen](#) auf Seite 686

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 Erfassung 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 gespeichert 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.

Zugehörige Konzepte

[Erfassung von Verbindungsdaten](#) auf Seite 685

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)
- 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

23.2.2 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 Tariffaktor. 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.

23.2.4 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:

Feldposit	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

Feldposit	Länge	Beschreibung
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:

Feldposit	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
15	1	PRI WATS-Band
16	3	PRI CIC

Feldpositio	Länge	Beschreibung
17	25	Gewählte oder empfangene Rufnummer (optional)

Anmerkung: In *HKEY_LOCAL_MACHINE\SOFTWARE* muss in den Registrierungsschlüsseln für *Accounting Tool* der Wert von **DateFormat DWORD** auf 1 festgelegt werden, um das nordamerikanische Datumsformat (MM.TT.JJ) zu erhalten. Standardwert ist 0 und steht für das in Europa und Lateinamerika verwendete Datumsformat (TT.MM.JJ).

Anmerkung: Die Datensätze von Accounting Manager in komprimierter Form sind durch das Trennzeichen | getrennt. Dies kann nur über Manager E konfiguriert werden.

Unkomprimiertes Format

Das unkomprimierte Format eignet sich für Ausdrücke. Außerdem wird eine Kopfzeile und Seitenvorschub ausgegeben. Ein Verbindungsdatensatz im komprimierten Format enthält folgende durch | getrennte Felder:

Feldpositio	Zeichenpositio 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

Feldpositio	Zeichenpositio Länge	Beschreibung
8	74-84 (11)	<p>Tarifeinheiten für einen Verbindungsabschnitt: zzzzzzzzzzzz (z = Ziffer: Wertebereich 0 ... 9)</p> <p>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.</p> <p>Für die Einstellung des Tariffaktors gilt:</p> <ul style="list-style-type: none"> • Mit Rechengenauigkeit: Tariffaktor = 100% + evtl. notwendiger Aufschlag • Ohne Rechengenauigkeit: Tariffaktor = Betrag/Einheit + evtl. notwendiger Aufschlag <p>In Abhängigkeit von der Rechengenauigkeit erfolgt die Erfassung der Verbindungskosten mit oder ohne Aufschlag:</p> <p>Die Ausgabe erfolgt immer, wenn für den Verbindungsabschnitt Verbindungskosten anfallen (z.B. auch bei übergebenen Verbindungen).</p>

Feldpositio	Zeichenpositio Länge	Beschreibung
9	85-86 (2)	<p>Informationselement: zusätzliche Information</p> <p>Wertebereich 0 ... 9</p> <p>Bedeutung:</p> <ul style="list-style-type: none"> • 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). • +10 = Offset als Kennung für Anrufe in Blacklist • +20 = Offset als Kennung für Kosten für den Verbindungsaufbau (ohne Verbindungsdauer) • +30 = Offset als Kennung für einen Folgedatensatz bei <ul style="list-style-type: none"> - 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)	<p>Vom Benutzer für diese Verbindung eingegebene Projektkennzahl</p> <p>PKZ: ppppppppppp</p> <p>(p = Ziffer der PKZ: Wertebereich 0 ... 9)</p> <p>Fehlende Ziffern werden durch Leerzeichen ersetzt.</p>
11	98-108 (11)	<p>Benutzte MSN: mmmmmmmmmmm</p> <p>(m = Ziffer der MSN: Wertebereich 0 ... 9)</p> <p>Die Anzeige erfolgt, sofern der Teilnehmer eine MSN-Taste programmiert hat.</p> <p>Bei gehenden Verbindungen eines MULAP-Teilnehmers wird die Rufnummer der belegten MULAP ausgegeben.</p> <p>Fehlende Ziffern werden durch Leerzeichen ersetzt.</p>

Feldpositio	Zeichenpositio Länge	Beschreibung
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-Kopf	Anforderungsmethode = GET
URL	https://<IP-Adresse des Systems>/management/portlet
Parameter	portlet=hipath-accountingdownload::HiPathAccountingDownloadPortlet entity=accounting action=get username=<username> password=<password>

Anmerkung: Beim Zugriff auf Gebührendaten mit der referenzierten Schnittstelle gelten die Einschränkungen der HTTP GET-Anforderung. Die folgenden Sonderzeichen dürfen nicht als Passwort verwendet werden, wenn jemand versucht, Daten über eine URL-Anfrage zu erhalten:

:/?#[]@ ! \$ & ' () * + , ; =

Beispiel:

```
https://192.148.108.151/management/portlet/?portlet=hipath-accountingdownload::HiPathAccountingDownloadPortlet&entity=accounting&action=get&username=xbert@system&password=not4u;-)
```

Download Response – Definition

Element	Inhalt
HTTP-Kopf	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-Kopf	Anforderungsmethode = 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::HiPathAccountingDownloadPortlet&entity=accounting&action=get&username=xbert@system&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

Zugehörige Konzepte

[Accounting-Tools](#) auf Seite 697

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.

23.3.2 Schutz vor Gebührenbetrug

Das System kann Verbindungen überwachen, um einen potenziellen Gebührenbetrug zu erkennen (Toll Fraud Monitoring). Dies betrifft Verbindungen, die über eine Amtsleitung ankommen und wieder 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.

23.4 Accounting-Tools

Accounting Tools bietet Accounting Manager und Teledata Office.

Zugehörige Konzepte

[Service Center – Dokumente](#) auf Seite 86

[Übertragung von Verbindungsdaten](#) auf Seite 689

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 Schnittstelle für Verbindungsdaten verwenden. Sie können Accounting Manager im **Service Center** des WBM herunterladen. Accounting Manager erfordert lokale Administrationsrechte und die Aktivierung von TLS 1.2 in Microsoft Internet Explorer.

23.4.2 Teledata Office

Teledata Office ist eine Windows-Anwendung für die Auswertung von Verbindungsdaten.

24 Wartung

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 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.

24.1.2 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.

24.1.3 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.

Zugehörige Konzepte

[Update der Systemtelefone](#) auf Seite 712

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 >

24.1.5 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.

Zugehörige Konzepte

[Konfiguration der Teilnehmer](#) auf Seite 225

Zugehörige Tasks

[Wie Sie IP- und SIP-Teilnehmer konfigurieren](#)

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.

24.1.7 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:

- Wartemusik (MOH)
- EXMR

Siehe Installation OpenScape Business X1/X1W, Service Dokumentation oder Installation OpenScape Business X3/X5/X8, Service Dokumentation.

- MUSIC Einsteckmodul
Siehe Installation OpenScape Business X1/X1W, 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.

Anmerkung: Bitte vergewissern Sie sich vorher, dass Sie mit der Benutzung von Ansagen oder Wartemusik keine Copyright-Verletzungen begehen.

Wichtig: Wenn der gehaltene Teilnehmer ein IP Workpoint Client oder ein IP-Trunk ist, wird die interne MOH verwendet. Externe MOH ist für IP nicht vorgesehen.

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**

Wartemusik (MOH)

Für Tag - und Nachtbetrieb (Nachtschaltung) kann unterschiedliche Wartemusik konfiguriert werden.

Anmerkung: Bei UC Suite gibt es keinen Unterschied zwischen Tag- und Nachtdateien. Die **Wartemusik-Datei - Tag** wird verwendet.

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 das Freizeichen.

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. beim Halten oder während ein Teilnehmer besetzt ist oder gerade 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 eine einzelne (Start / Stopp) oder die kontinuierliche Wiedergabe konfigurieren.

Anmerkung: In eingebetteten Systemen wird der kontinuierliche Modus nicht unterstützt.

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.

Anmerkung: Bitte vergewissern Sie sich vorher, dass Sie mit der Benutzung von Ansagen oder Wartemusik keine Copyright-Verletzungen 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**

24.1.9 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 Leistungsmerkmal 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 #.

24.2 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.

Anmerkung: 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.

Jedes Backup wird mit einem systemspezifischen Schlüssel verschlüsselt.

Ein verschlüsseltes Backup-Set kann nur für die Wiederherstellung des Systems verwendet werden, von dem das Backup verschlüsselt wurde.

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-Set 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 "Harddisk" 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-Set
- **Größe:** Größe des Backup-Sets in Byte.
- **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.

24.2.2 Backup-Medien

Auf den Backup-Medien werden die Backup-Sets gesichert.

Für die Sicherung können folgende Backup-Medien verwendet werden:

- Gestecktes USB-Medium
- Network drive

- Client-PC über HTTPS (nur möglich bei sofortiger Sicherung)
- Festplatte der UC Booster Card
- FTP-/FTPS-Server

Für jedes Backup-Medium kann festgelegt werden, wie viele 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. Aufgrund der Dateisystembeschränkung darf die maximale Größe des Backup-Sets 4 GB nicht überschreiten. In solchen Fällen müssen alternative Backup-Medien ausgewählt werden. Von 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 TLS 1.2 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 erforderlich.

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 **Local 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 ebenfalls abgespeichert werden muss. Um das Backup-Set bei einer möglichen Wiederherstellung leichter identifizieren zu können, kann ein Kommentar angegeben werden.

Zugehörige Konzepte

[Zeitgesteuertes Sichern](#) auf Seite 708

Zugehörige Tasks

[Wie Sie das eigene Administratorpasswort ändern](#)

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.

Zugehörige Konzepte

[Sofortiges Sichern](#) auf Seite 707

24.2.5 Wiederherstellen

Die Wiederherstellung der Konfigurationsdaten erfolgt manuell über die Backup-Sets.

Die Wiederherstellung kann von allen unterstützten Backup-Medien erfolgen.

24.3 Updates

Mit Hilfe von Updates wird die Software der Systemkomponenten innerhalb einer Version aktualisiert.

Um Updates installieren zu können, benötigen Sie den 3 jährigen Software-Support.

Die Version der installierten Software und das Ablaufdatum des Software-Supports werden auf der Startseite des WBM angezeigt. Ist eine aktuellere Software verfügbar, wird dies dort mitgeteilt.

Anmerkung: 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 einem Hardwaremodell 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 Hardwaremodell 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.

Das Software-Update kann sofort gestartet werden oder die Zeitpunkte für die 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.

Anmerkung: Das Software-Update muss nicht gleichzeitig auf allen Systemen und in verschiedenen Software-Versionen durchgeführt werden.

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 Systemteletyp 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.

24.3.2 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 ([Sicherung und Wiederherstellung](#)).

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 ausgewählt 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.

24.3.3 Update der Systemtelefone

Die Software der Systemtelefone wird über eine Image-Datei aktualisiert. Für jeden Systemteletyp 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. Wird ein IP-Systemtelefon im WBM umkonfiguriert (von einem System Client zu einem SIP Client oder umgekehrt) wird automatisch über den DLI die passende, im Kommunikationssystem gespeicherte Software auf das IP-Systemtelefon geladen. Bei IP-Systemtelefonen, die bereits am System oder an einem anderen System in Betrieb waren, müssen zuerst die Werkseinstellungen wiederhergestellt werden (Factory Reset), bevor die automatische Software-Aktualisierung durchgeführt werden kann.

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).

Zugehörige Konzepte

[Telefon-Logos](#) auf Seite 700

24.3.4 Software-Status

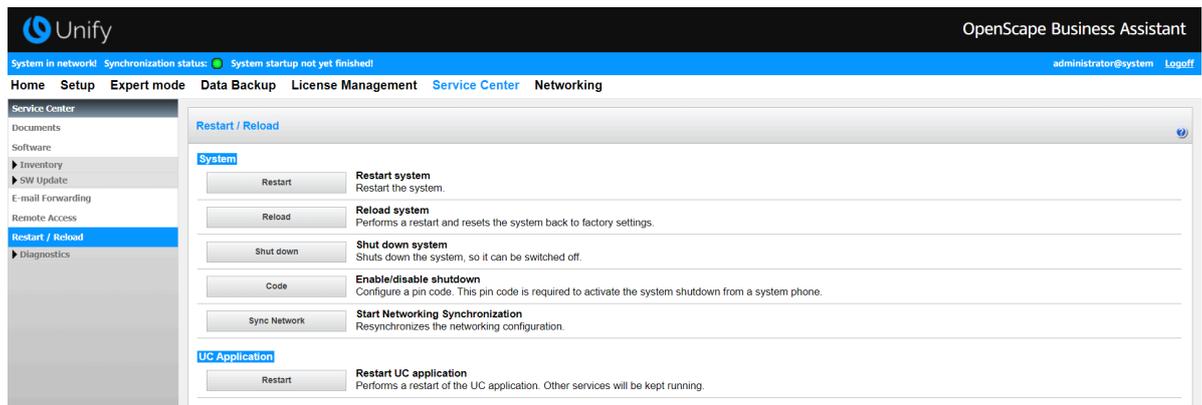
Der Software-Status gibt Auskunft über den Softwarestand und die Aktualisierung der Software.

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

24.4 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 reloaded 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.

24.4.2 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.

24.4.3 Shutdown (Herunterfahren) von OpenScape Business X

Über die Funktion **System herunterfahren** kann ein kontrolliertes Herunterfahren der Kommunikationssysteme OpenScape Business X veranlasst werden.

24.4.4 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**.

24.4.5 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 werden die CSTA-Schnittstelle, der Presence Manager, das Wiedergabegerät für Ansagen, die Media Extension Bridge und der Open Directory Service ebenfalls neu gestartet.

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](#)).

24.4.7 Restart (Neustart) der UC Applikation

Über die Funktion **UC Applikation 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 und myAttendant, getrennt. Nach dem Hochlauf werden alle Verbindungen automatisch wiederhergestellt.

24.5 Inventory-Management

Unter Inventory-Management versteht man die Ermittlung des aktuellen Status der Kommunikationssysteme OpenScape Business X und 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
- Gerätetyp
- 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 Telekommunikationsnetzte) 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 werden durch die Farbe des zugehörigen Rechtecks angezeigt (grün = OK, 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 wird angezeigt, über welchen Wizard und über welche Menüs im Experten-Modus die IP-Adressen konfiguriert werden können.

Es wird außerdem eine Statusübersicht der Booster Card und Mainboard Ethernet-Schnittstellen angezeigt.

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

Wartung

Automatische Aktionen

- 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
- Übersicht über alle Booster-Card-Schnittstellen

Der Link **UC Booster Card erreichbar** auf der Startseite des WBM leitet den Benutzer zu einer Detail-Ansicht unter **Service-Center > Inventory > Booster-Karte** weiter. Der Link existiert auch dann, wenn es ein Problem mit der Booster Card gibt und die Nachricht **UC Booster Card nicht erreichbar** angezeigt wird.

Die folgenden Fehlermeldungen werden auf der Startseite des WBM angezeigt:

- 1) Inter-Integrated Circuit-Verbindung mit Booster Card nicht möglich
- 2) Internet Protocol v6 Konnektivität mit Booster Card nicht möglich
- 3) Internet Protocol v4 Konnektivität mit Booster Card nicht möglich
- 4) Secure Socket Shell (SSH) Konnektivität mit Booster Card nicht möglich
- 5) Network File System (NFS) Konnektivität mit Booster Card nicht möglich
- 6) Eine bzw. mehrere Ethernet-Schnittstellen befinden sich im Halbduplex-Modus; Vollduplex dringend empfohlen

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.

24.6 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.

24.6.2 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.

24.6.3 Warnmechanismus für SDHC-Kartenlebensdauer

Die automatische Aktion Warnmechanismus für die SDHC-Lebensdauer ist eine Möglichkeit, Informationen über den Zustand der SDHC-Karten mit einer Dateisystemprüfung während des Startvorgangs abzurufen. Ein WBM-Wizard wird gestartet und führt den Techniker durch die Festlegung einer Zeit, zu der das System einen Neustart durchführen und die Prüfung ausführen soll.

Anmerkung: Falls bei der Überprüfung keine Dateisystemfehler gefunden werden, wird **SDHC-Integritätsstatus** wieder auf grün oder gelb gesetzt, auch wenn zuvor Fehler gemeldet wurden.

Alle Informationen werden im Kunden-Trace protokolliert. In der Standardeinstellung ist die automatische Aktion Warnmechanismus für SDHC deaktiviert.

Anmerkung: Diese Option löst einen Neustart des Systems aus, während die folgende Warnung angezeigt wird "Hinweis: Das System wird neu gestartet, nachdem Sie "OK" drücken."

Die WBM-Startseite erkennt zwei Zustände:

- Wenn die Informationen im System verfügbar sind, wird ein Text auf dem Startbildschirm angezeigt, der über den allgemeinen Status der Karte informiert: **SDHC-Integritätsprüfung** (grün, gelb, rot oder grau).

Die allgemeine Lebensdauer der Karte wird basierend auf den Herstellerspezifikationen und den durchschnittlichen Schreibzyklen des Systems berechnet. Es sind unterschiedliche Werte für die Lebensdauer der Karte möglich. Diese Informationen werden zusammen mit anderen Informationen auf der Seite „SDHC-Integritätsprüfung“ im WBM angezeigt.

Eine geschätzte Lebensdauer von 4 Jahren für Standardkarten und 10 Jahren für Karten mit hoher Ausdauer wird innerhalb des Systems gespeichert.

Anmerkung: Die geschätzten Werte für die Lebensdauer sind nur die Basis für den Warnmechanismus der integrierten SDHC-Integritätsprüfung. Diese Werte implizieren nicht automatisch, dass eine Karte nach Ablauf dieser Zeit defekt ist.

Ein grüner Integritätsstatus zeigt an, dass die Karte ihre geschätzte Lebensdauer nicht erreicht hat und es ein Problem mit dem Dateisystem gibt.

Ein gelber Integritätsstatus zeigt an, dass die Karte ihre geschätzte Lebensdauer erreicht.

Ein roter Integritätsstatus zeigt an, dass mehr als 50 Dateisystemfehler gefunden wurden.

Ein grauer Integritätsstatus zeigt an, dass die Karte entweder nicht unterstützt wird oder keine Informationen für die Karte abgerufen werden können. Die SDHC-Karte muss durch einen unterstützten Typ ersetzt werden.

Der Warnmechanismus für den gelben Integritätsstatus basiert auf dem Herstellungsdatum und der geschätzten Lebensdauer der Karte. Da Karten länger vorrätig sein können, bis sie in OpenScape Business verwendet werden, wird das Erstellungsdatum des Dateisystems ebenfalls im Berechnungsalgorithmus berücksichtigt.

Im Folgenden wird eine Berechnungstabelle für die SDHC-Integritätsprüfung mit einer geschätzten Lebensdauer von 4 Jahren angezeigt.

Faktor	Jahre und Gewichtung									
	Herstellungsdatum Jahre	< 5 Jahre		< 6 Jahre		< 7 Jahre		< 8 Jahre		> 8 Jahre
Dateisystem erstellt	< 4 years	< 4 years	4-5 Jahre	< 4 years	4 - 6 Jahre	< 3 Jahre	3-7 Jahre	< 2 Jahre	2 - 8 Jahre	-
SDHC-Integritätsstatus	Grün	Green	Gelb	Green	Yellow	Green	Yellow	Green	Yellow	Yellow

- Falls die Informationen nicht verfügbar sind, erhält der Benutzer die folgende Meldung: **Card Health Status unknown.**

Anmerkung: Ist das Dateisystem beschädigt, muss das entsprechende System-SW-Image von SWS heruntergeladen und mit dem Card Manager Tool auf die SDHC-Karte kopiert werden. Nach dem Start des Systems mit der neuen SDHC-Karte kann die Konfiguration mit der neuesten Sicherung wiederhergestellt werden.

Der Text „**Card Health Status**“ enthält auch einen Link, der zur Seite "Aktionen" führt.

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

Wartung

Überwachung und Wartung von OpenScape Business

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.

24.8 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.

24.8.2 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.

Anmerkung: 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: Kritisch: 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. Gelöscht 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	-
Uhrzeit	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.

SNMP-Code	Event-Log-Eintrag	Bedeutung	Erforderliche Maßnahmen	Hinweis
Fehlerklasse 01 - Allgemeine Meldungen				
	Restart des Systems	Harter Neustart (Reset) des gesamten Systems mit aktuellem KDS.	Keine	
FP_EVT_ADM_002	Nachladen des signierten Slots	Nachladen des signierten Slots		
FP_EVT_ADM_003	Restart des Systems	Restart des Systems		
FP_EVT_ADM_010	Restart des SNMP Systems	Harter Neustart des gesamten Systems über SNMP.	Keine	
FP_EVT_ADM_014	SNMP lokale DB-Änderungen	Vor-Ort-Änderungen an der Datenbank.	Keine	
FP_EVT_ADM_015	SNMP Remote-DB-Änderungen	„Remote“-Änderungen an der Datenbank.	Keine	
FP_EVT_ADM_016	SNMP APSXF-Ergebnis	APS-Übertragungsbestätigungsnachricht über SNMP.	Keine	
FP_EVT_ADM_017	SNMP-Authentifizierung fehlgeschlagen	Unerlaubter Zugriffsversuch.	Überprüfen Sie die Firewall-Einstellungen in OpenScape Business/ Manager E (Netzwerk Firewall).	
FP_EVT_ADM_019	Sensor-Alarm	Die Temperatur im OpenScape Business-Gehäuse ist zu hoch.	Überprüfen Sie das Gebläse und die Luftzufuhr im 19-Zoll-Gehäuse. Beachten Sie die Umgebungstemperatur.	
FP_EVT_ADM_020	CDR-Puffergrenze erreicht	Überlauf im CDR-Puffer (CDR-Informationen).	Prüfen Sie, ob die Schnittstellen (V.24, LAN), Ports und die Verbindung funktionieren oder lesen Sie die Rufdaten aus.	
FP_EVT_ADM_024	unautorisierte Applikation	Versuchter Zugriff über eine nicht autorisierte Applikation.	Überprüfen Sie die Firewall-Einstellungen in OpenScape Business/ Manager E (Netzwerk Firewall).	

Wartung

SNMP-Code	Event-Log-Eintrag	Bedeutung	Erforderliche Maßnahmen	Hinweis
FP_EVT_ADM_025	Manual Switchback aus HiPath Manager			
Fehlerklasse 02 - Meldungen zur Lizenzverwaltung				
Fehlerklasse 09 - Hardware-Modul-Meldungen				
FP_EVT_HW_034	Verlust des Rahmens ein (STMD)	Verlust des Rahmens ein (STMD)		
FP_EVT_HW_035	Verlust des Rahmens aus (STMD)	Verlust des Rahmens aus (STMD)		
FP_EVT_HW_036	Schlupf erkannt ein (STMD)	Auf einer ISDN-Leitung ist ein Bitfehler aufgetreten.	Überprüfen Sie die S0-Leitung. Falls erforderlich, laden Sie die Baugruppe neu oder führen Sie einen harten Neustart durch. Wenn der Fehler weiterhin besteht, richten Sie einen ISDN-Trace ein.	Das Problem kann durch asynchrone interne und externe Taktraten verursacht werden. Datenverlust möglich/Verbindung kann unterbrochen werden.
FP_EVT_HW_039	Alarmanzeige Signalfehler aus (TMS2M)	Alarmanzeige: Der S2M-Fehler ist korrigiert worden.	Keine	
FP_EVT_HW_040	degradierter Minutenfehler ein (TMS2M)	degradierter Minutenfehler ein (TMS2M)		
FP_EVT_HW_041	degradierter Minutenfehler aus (TMS2M)	degradierter Minutenfehler aus (TMS2M)		
FP_EVT_HW_042	kein Signalfehler ein (TMS2M/STMD)	Alarmanzeige: Ein S2M-Fehler ist aufgetreten. Keine physische Verbindung vorhanden.	Überprüfen Sie die S2M-Leitung und die Baugruppe. Falls erforderlich, laden Sie die Baugruppe neu oder führen Sie einen harten Neustart durch. Wenn der Fehler weiterhin besteht, richten Sie einen ISDN-Trace ein.	

SNMP-Code	Event-Log-Eintrag	Bedeutung	Erforderliche Maßnahmen	Hinweis
FP_EVT_HW_043	kein Signalfehler aus (TMS2M/STMD)	Alarmanzeige: Der S2M-Fehler ist korrigiert worden.	Keine	
FP_EVT_HW_046	schwer fehlerhafte Sekundenfehler ein(TMS2M)	schwer fehlerhafte Sekundenfehler ein(TMS2M)		
FP_EVT_HW_047	schwer fehlerhafte Sekundenfehler aus (TMS2M)	schwer fehlerhafte Sekundenfehler aus (TMS2M)		
FP_EVT_HW_052	Uhr kann als Ref. verwendet werden (TMS2M/STMD)	Uhr kann als Ref. verwendet werden (TMS2M/STMD)		
FP_EVT_HW_053	Uhr kann nicht als Referenz verwendet werden	Uhr kann nicht als Referenz verwendet werden		
FP_EVT_HW_060	Zugriff auf Einspeisefehler ein (SLMO)	Zugriff auf Einspeisefehler ein (SLMO)		
FP_EVT_HW_063	ELIC-Fehler ein (SLMO/SLMC)	ELIC-Fehler ein (SLMO/SLMC)		
FP_EVT_HW_064	ELIC-Fehler aus (SLMO/SLMC)	ELIC-Fehler aus (SLMO/SLMC)		
FP_EVT_HW_067	OCTAT-Fehler ein (SLMC)	OCTAT-Fehler ein (SLMC)		
FP_EVT_HW_096	unbekannter Fehler von LW	unbekannter Fehler von LW		
Fehlerklasse 11 - Allgemeine Meldungen				
FP_EVT_DEV_041	L1 asynchron ein	L1 asynchron ein		
FP_EVT_DEV_042	L1 asynchron aus	L1 asynchron aus		
FP_EVT_DEV_043	Überlastungsfehler ein	Überlastungsfehler ein		
FP_EVT_DEV_044	Überlastungsfehler aus	Überlastungsfehler aus		
FP_EVT_DEV_045	Alive-Check-Fehler ein	Alive-Check-Fehler ein		
FP_EVT_DEV_046	optiPoint-Informationen	optiPoint-Informationen		
FP_EVT_DEV_048	Layer-2-Fehler erkannt	Layer-2-Fehler erkannt		
FP_EVT_DEV_049	Layer-3-Fehler erkannt	Layer-3-Fehler erkannt		
FP_EVT_DEV_052	Andere Fehler	Andere Fehler		
FP_EVT_DEV_057	KEIN TEI verfügbar	KEIN TEI verfügbar		

Wartung

SNMP-Code	Event-Log-Eintrag	Bedeutung	Erforderliche Maßnahmen	Hinweis
FP_EVT_DEV_058	Zu viele L1-Fehler	Zu viele Layer-1-Fehler.	Überprüfen Sie die Leitungen, das Endgerät und den Anschluss. Möglicherweise ist ein Kurzschluss aufgetreten.	
FP_EVT_DEV_059	Zugang nicht konfiguriert	Zugang nicht konfiguriert		
Fehlerklasse 16 - Betriebssystem-Meldungen				
FP_EVT_GEN_002	Fehler im Freigabepool	Fehler im Freigabepool	Richten Sie einen Trace anhand der Informationen von BLS (Back Level Support) ein. Erstellen Sie einen Stack-Dump. Speichern Sie einen Snapshot.	
FP_EVT_GEN_004	Fehler in OSF-Send	Fehler in OSF-Send	Richten Sie einen Trace anhand der Informationen von BLS (Back Level Support) ein. Erstellen Sie einen Stack-Dump. Speichern Sie einen Snapshot.	
FP_EVT_GEN_005	Fehler im OSF-Timer	Fehler im OSF-Timer	Richten Sie einen Trace anhand der Informationen von BLS (Back Level Support) ein. Erstellen Sie einen Stack-Dump. Speichern Sie einen Snapshot.	

SNMP-Code	Event-Log-Eintrag	Bedeutung	Erforderliche Maßnahmen	Hinweis
FP_EVT_GEN_010	RESTARTED: manueller Reset	RESTARTED: manueller Reset	Richten Sie einen Trace anhand der Informationen von BLS (Back Level Support) ein. Erstellen Sie einen Stack-Dump. Speichern Sie einen Snapshot.	
FP_EVT_GEN_011	RESTARTED: manueller Reload	RESTARTED wegen manuellem Reload	Richten Sie einen Trace anhand der Informationen von BLS (Back Level Support) ein. Erstellen Sie einen Stack-Dump. Speichern Sie einen Snapshot.	
FP_EVT_GEN_012	RESTARTED: Ausschalten	RESTARTED aufgrund eines Stromausfalls	Richten Sie einen Trace anhand der Informationen von BLS (Back Level Support) ein. Erstellen Sie einen Stack-Dump. Speichern Sie einen Snapshot.	
FP_EVT_GEN_013	KDS-Sicherung nicht durchgeführt	KDS-Sicherung nicht durchgeführt	Richten Sie einen Trace anhand der Informationen von BLS (Back Level Support) ein. Erstellen Sie einen Stack-Dump. Speichern Sie einen Snapshot.	

Wartung

SNMP-Code	Event-Log-Eintrag	Bedeutung	Erforderliche Maßnahmen	Hinweis
FP_EVT_GEN_014	RESTARTED: unbekannter Rest. Nichtübereinst. HW- Angabe	RESTARTED wegen unbekanntem Rest. Nichtübereinst. HW- Angabe	Richten Sie einen Trace anhand der Informationen von BLS (Back Level Support) ein. Erstellen Sie einen Stack-Dump. Speichern Sie einen Snapshot.	
FP_EVT_GEN_015	Allgemeines Fehlerprotokoll	Allgemeines Fehlerprotokoll	Richten Sie einen Trace anhand der Informationen von BLS (Back Level Support) ein. Erstellen Sie einen Stack-Dump. Speichern Sie einen Snapshot.	
FP_EVT_GEN_020	CSTA: Länge außerhalb des Bereichs	CSTA: Länge außerhalb des Bereichs	Richten Sie einen Trace anhand der Informationen von BLS (Back Level Support) ein. Erstellen Sie einen Stack-Dump. Speichern Sie einen Snapshot.	
FP_EVT_GEN_024	Leerlauf nach Neustart eingetroffen	Leerlauf nach Neustart eingetroffen	Richten Sie einen Trace anhand der Informationen von BLS (Back Level Support) ein. Erstellen Sie einen Stack-Dump. Speichern Sie einen Snapshot.	

SNMP-Code	Event-Log-Eintrag	Bedeutung	Erforderliche Maßnahmen	Hinweis
FP_EVT_GEN_030	Überschreit. CSTA-Monitor-Pkte.	Überschreit. CSTA-Monitor-Pkte.	Richten Sie einen Trace anhand der Informationen von BLS (Back Level Support) ein. Erstellen Sie einen Stack-Dump. Speichern Sie einen Snapshot.	
Fehlerklasse 19 - Meldungen der Netzwerkdienste				
FP_EVT_NWS_011	SNTP-Client am PCS kann nicht aktiviert werden	SNTP-Client am PCS kann nicht aktiviert werden		
Fehlerklasse 20 - Meldungen der Anrufverarbeitung				
FP_EVT_CP_002	RS232: DSR nicht bereit	Die RS232/V.24-Schnittstelle ist defekt.	Überprüfen Sie die Schnittstelle, die Leitung und die Applikation.	
FP_EVT_CP_013	nicht verbundene Wege	Die maximal zulässige Anzahl von Verbindungswegen wurde überschritten.	Verwenden Sie das Projektierungswerkzeug, um die Systemkonfiguration zu testen. Richten Sie einen Trace mit Informationen von BLS ein. Erstellen Sie einen Stack-Dump. Speichern Sie einen Snapshot.	
Fehlerklasse 21 - Geräte-Handler-Meldungen				
FP_EVT_DH_004	Port außer Betrieb	Port außer Betrieb		
FP_EVT_DH_005	Port betriebsbereit	Port betriebsbereit		
FP_EVT_DH_016	Name in S0/S2M msg verwerfen	Name in S0/S2M msg verwerfen		
FP_EVT_DH_017	Meldung zu lang L3S int->ext	Meldung zu lang L3S int->ext		
FP_EVT_DH_018	Meldung zu lang L3S ext->int	Meldung zu lang L3S ext->int		
FP_EVT_DH_022	Auto PRI-Erkennung DMS250-Prot	Auto PRI-Erkennung DMS250-Prot		

Wartung

SNMP-Code	Event-Log-Eintrag	Bedeutung	Erforderliche Maßnahmen	Hinweis
FP_EVT_DH_023	Auto PRI-Erkennung NI2-Prot		Auto PRI-Erkennung NI2-Prot	I
FP_EVT_DH_024	Automatische PRI-Erkennung 4ESS-Protokoll		Automatische PRI-Erkennung 4ESS-Protokoll	
FP_EVT_DH_026	Überlauf des Schlüsselmoduls	Überlauf des Schlüsselmoduls		
FP_EVT_DH_027	B-chan-Grenze erreicht	B-chan-Grenze erreicht		
Fehlerklasse 23 - Geräte-Handler-Meldungen				
FP_EVT_NW_060	Systemhalt, kein Puffer verfügbar	Systemhalt, kein freier Puffer mehr verfügbar.	Richten Sie einen Trace mit Informationen von BLS ein. Erstellen Sie einen Stack-Dump. Speichern Sie einen Snapshot.	
Fehlerklasse 26 - Meldungen der Baugruppenadministration				
FP_EVT_PR_001	Karte außer Betrieb	Die angegebene Baugruppe ist außer Betrieb.	Keine	
FP_EVT_PR_003	anderer Kartentyp als alter Kartentyp	Inkompatibler Kartentyp. Der Steckplatz ist bereits mit einem anderen Baugruppentyp vorbelegt.	Tauschen Sie die Baugruppe aus oder löschen Sie mit dem Assistenten T den voreingestellten Baugruppentyp, damit die neue Baugruppe erkannt wird.	
FP_EVT_PR_004	Karte betriebsbereit	Die angegebene Karte ist betriebsbereit.	Keine	
FP_EVT_PR_005	Fehler beim Lesen der Datenbank	Fehler beim Lesen der Datenbank		
Fehlerklasse 28 - Wiederherstellungsmeldungen				
FP_EVT_RC_008	Fehlende APS im EventLog B	Fehlende APS im EventLog B	Keine	Die aktuelle APS-Version wird beim Kopieren des EventLogs B eingetragen. Dies erleichtert die Analyse.
Fehlerklasse 30 - Board-Software-Meldungen				

SNMP-Code	Event-Log-Eintrag	Bedeutung	Erforderliche Maßnahmen	Hinweis
FP_EVT_LW_095	keine USB-Verbindung zum System	keine USB-Verbindung zum System		
Meldungen zum Ressourcenmanager				
FP_EVT_RM_001	Resource Manager Fehlerkonfiguration	Resource Manager Fehlerkonfiguration		
Nachrichten zum UPM				
FP_EVT_UPM_010	UPM: neu gestartet	UPM: neu gestartet		

SNMP-Code	Event-Log-Eintrag	Bedeutung	Erforderliche Maßnahmen	Hinweis
MSG_DLSC_BOOTSTRAP_OK	DLS-Client erfolgreich gebootstrapt.	DLS-Client erfolgreich gebootstrapt.		
MSG_STRC_STOP	Sicherer Trace gestoppt.	Sicherer Trace gestoppt.		
MSG_STRC_START	Sicherer Trace gestartet für Protokolle.	Sichere Traces wurden vom Benutzer für die genannten Protokolle aktiviert.		
MSG_SPE_CERT_MISSING	SPE-Zertifikat fehlt.	Kein SPE-Zertifikat installiert.	SPE-Zertifikat und privaten Schlüssel importieren (Datei PKCS#12).	
MSG_SPE_CERT_AVAIL	SPE-Zertifikat vorhanden.	SPE-Zertifikat ist jetzt verfügbar.		
MSG_SPE_CERT_UPDATED	Das SPE-Zertifikat wurde erfolgreich aktualisiert.	Das SPE-Zertifikat wurde erfolgreich aktualisiert.		
MSG_SPE_CERT_EXPIRED	SPE-Zertifikat abgelaufen.	Die Gültigkeitsdauer des installierten SPE-Zertifikats ist abgelaufen.	Installieren Sie ein neues gültiges Zertifikat.	
MSG_SPE_CRL_EXPIRED	Die SPE CRL für eine bestimmte CA ist abgelaufen.	CDP unzugänglich oder abgerufene CRL ist abgelaufen.	Importieren Sie ein in CDP konfiguriertes SPE CA-Zertifikat mit gültigen CRLs.	
MSG_SPE_CRL_UPDATED	Die SPE CRL für CA wurde erfolgreich aktualisiert.	Die SPE CRL für CA wurde erfolgreich aktualisiert.		
MSG_SPE_ALL_CRLS_UPTODATE	Alle SPE CRLs sind wieder auf dem neuesten Stand.	Alle SPE CRLs sind wieder auf dem neuesten Stand.		

Wartung

SNMP-Code	Event-Log-Eintrag	Bedeutung	Erforderliche Maßnahmen	Hinweis
MSG_MIKEY_REBOOT	Mikey Stack: Durchsetzung gescheitert.	Mikey Stack: Durchsetzung gescheitert.		
MSG_IPSEC_REBOOT	Fataler Fehler im IPSec-Stack.	Fataler Fehler im IPSec-Stack.		
MSG_CAT_H323_REBOOT		Neustart mit H.323		
MSG_CAT_HSA_REBOOT		Neustart mit HAS		
MSG_GW_SUCCESSFULLY_STARTED				
MSG_IP_LINK_FAILURE				
MSG_IP_LINK2_FAILURE		IP-Link 1 auf/ab		
MSG_IP_LINK3_FAILURE				
MSG_NEW_SW_AVAILABLE				
MSG_ADMIN_NEUSTART		Neustart mit WBM/CLI- Admin, Software- Upgrade oder Datenwiederherstellung		
MSG_SYSTEM_NEUSTART		Automatischer Neustart, zum Beispiel mit Garbage Collection		
MSG_EXCEPTION_REBOOT		Neustart mit SW- Ausnahme		
MSG_GW_OBJ_MEMORY_EXHAUSTED		Kein Speicherplatz vorhanden		
MSG_TLS_POOL_SIZE_EXCEEDED		Keine internen Pools mehr		
MSG_OAM_RAM_THRESHOLD_REACHED		RAM-Grenze erreicht		
MSG_OAM_DMA_RAM_THRESHOLD_REACHED		DRAM-Grenze erreicht		
MSG_OAM_THRESHOLD_REACHED		Limit erreicht, zum Beispiel für Flash- Speicher oder IP- Pools		
MSG_OAM_HIGH_TEMPERATURE_EXCEPTION		Temperaturgrenze erreicht (zu heiß)		
MSG_HACKER_AUF_SNMP_PORT_TRAP		Unerlaubter Zugriff auf SNMP-Port		
MSG_DVMGR_LAYER2_SERVICE_TRAP		B-Kanal auf/ab		

SNMP-Code	Event-Log-Eintrag	Bedeutung	Erforderliche Maßnahmen	Hinweis
MSG_SSM_NUM_OF_CALL_LEGS_2BIG	Mehr als 2 Call-Legs: nicht unterstützt! CSID: %x/%x	Es sind nicht mehr als zwei Call-Legs pro Sitzung erlaubt. Dies hat dazu geführt, dass die Software instabil geworden ist. Der notwendige Neustart wird durchgeführt.		
MSG_SSM_SESSION_CREATION_FAILED	Sitzungserstellung fehlgeschlagen	Eine Signalisierung ist nicht mehr möglich, da eine Sitzung nicht aufgebaut werden konnte. Der notwendige Neustart wird durchgeführt. Es wird ein SNMP-Trap erzeugt.		
MSG_IPNCV_STARTUP_ERROR	IPNCV Startup: Erstellen des IPNCV-Managers fehlgeschlagen	IPNCV konnte nicht gestartet werden. Es wird ein SNMP-Trap erzeugt.	Einen TR/MR erstellen	
MSG_IPNCV_STARTUP_SHUTDOWN	IPNCV Start/Stop: IPNCV-Manager erfolgreich erstellt oder IPNCV starten/stoppen: IPNCV Manager erfolgreich heruntergefahren	IPNCV wurde erfolgreich gestartet oder gestoppt, ein SNMP-Trap wird erzeugt		
MSG_IPNCV_INTERNAL_ERROR	Interner IPNCV-Fehler: %s	Software-Fehler: ungültige interne Daten gefunden. Es wird ein SNMP-Trap mit dem Profil IPNCV- Detailed generiert.		
MSG_IPNCV_MEMORY_ERROR	IPNCV-Speicher: %s	Speicherüberlauf: Es wird ein SNMP-Trap erzeugt.	Gateway neu starten. Einen TR/MR erstellen.	
MSG_IPNCV_SIGNALING_ERROR	IPNCV-Signalfehler: %s	Softwarefehler: ungültige interne Daten gefunden.		
MSG_CAR_ALIVE_IP_CONNECTION_LOST	CAR: Alive: ip-Verbindung %d.%d.%d.%d verloren	CAR: Alive: IP-Verbindung verloren.		

SNMP-Code	Event-Log-Eintrag	Bedeutung	Erforderliche Maßnahmen	Hinweis
MSG_LIC_DATA_ACCEPTED		Lizenzdaten akzeptiert		
MSG_LIC_DATA_CORRUPTED		Lizenzdaten unvollständig		
MSG_LIC_DATA_NOT_ACCEPTED		Lizenzdaten akzeptiert		
MSG_SPE_CERT_MISSING	Kein SPE-Zertifikat installiert!	SPE-Zertifikat fehlt.	SPE-Zertifikat installieren.	

Anmerkung: Es gibt SNMP-Events, die in diesem Leitfaden nicht dokumentiert sind.

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	Erklärung	Anwendungsfall
Trace-Protokoll	<p>Standard-Trace-Datei, wenn Trace-Profil aktiviert werden.</p> <p>Zwischen folgenden Optionen kann gewählt werden:</p> <ul style="list-style-type: none"> • 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

Protokoll	Erklärung	Anwendungsfall
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
UC Suite-Protokolle	<p>Meldungen der UC Suite des Kommunikationssystems (UC Suite-, CSP- und MEB-Protokolle)</p> <p>Zwischen folgenden Optionen kann gewählt werden:</p> <ul style="list-style-type: none"> • 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. <p>Alle Protokolldateien werden in einer komprimierten Datei zusammengefasst. Für die OpenScape Business-Protokolle gelten folgende Dateibezeichnungen: UC Suite-Protokolldateien = vs_YYYY_MM_TT.log, CSP-Protokolldateien = csptrace_YYYY_MM_TT.log, MEB-Protokolldateien = mebtrace_YYYY_MM_TT.log.</p> <p>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.</p>	Probleme mit der UC Suite und/oder den Clients (myPortal for Desktop, myAttendant usw.)

Protokoll	Erklärung	Anwendungsfall
Applikationsprotokolle	<p>Meldungen des Applikationsanteils des Kommunikationssystems (zum Beispiel CSP-Protokolle)</p> <p>Ein Administrator mit dem Profil Expert kann über den Experten-Modus zwischen folgenden Optionen wählen:</p> <ul style="list-style-type: none"> • 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. <p>Alle Protokolldateien werden in einer komprimierten Datei zusammengefasst.</p>	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.

24.8.4 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.

Tipp:

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
- Uhrzeit
- Modulname
- 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.

Tipp:

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	<p>Datei-Trace aktivieren</p> <p>Trace-Meldungen werden im Kommunikationssystem in eine Protokolldatei eingetragen.</p> <p>Bei aktivierter Option gelten folgende Einstellungen:</p> <p>Max. Trace-Quota (kByte): Anzeige der maximalen Größe des Trace-Speichers</p> <p>Strategie bei Erreichen der max. Quota: Ausgewählt werden kann zwischen Wrap Around (Lösche älteste Datei) und Datei-Trace wird temporär gestoppt.</p> <p>Zeit, nach der jeweils eine neue Trace-Datei angelegt wird (s) 900</p> <p>Zeitraum für den Trace-Dateien verfügbar sind Die aktuelle Zeit wird angegeben.</p>	Aktiviert
Trace über LAN	<p>Trace über LAN aktivieren</p> <p>Trace-Meldungen werden über die LAN-Schnittstelle übertragen.</p> <p>Bei aktivierter Option gelten folgende Einstellungen: Timer-Wert = 25 s (Verzögerungszeit, bis Daten übertragen werden.)</p>	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.

Digital Loopback

Digitale Prüfschleifen werden zur Leitungsüberprüfung von B-Kanälen der S₀⁻, 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.

Anmerkung: Das Aufzeichnen von Gesprächen und Verbindungsdaten ist ein Straftatbestand, 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.

Anmerkung: 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	<p>Konsolen-Trace aktivieren</p> <p>H.323-Stack-Trace-Meldungen werden auf der Konsole ausgegeben.</p>	Nicht aktiviert
Datei-Trace	<p>Datei-Trace aktivieren</p> <p>H.323-Stack-Trace-Meldungen werden in eine Protokolldatei eingetragen.</p> <p>Bei aktivierter Option gelten folgende Einstellungen:</p> <p>Max. Größe des Trace-Buffers = 50000 Byte (Menge der Daten, die im Zwischenspeicher gehalten wird.)</p> <p>Max. Größe der Trace-Datei = 1000000 Byte (Maximale Größe der Protokolldatei.)</p> <p>Trace-Timer = 60 s (Verzögerungszeit, bis Daten in die Protokolldatei geschrieben werden.)</p>	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-Profilen 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-Profilen zur Verfügung, die alle Standardszenarien adressieren. Zusätzlich kann ein Administrator mit dem Profil **Expert** eigene Trace-Profilen anlegen. Durch Starten eines Trace-Profiles wird die Aufzeichnung über dieses Profil aktiviert und durch Stoppen deaktiviert.

- Ein Administrator mit dem Profil **Advanced** kann über den Wizard **Trace** Trace-Profilen starten und/oder stoppen. Der Status jedes Trace-Profiles 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-Profilen 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-Profilen gemeinsam stoppen und Trace-Profilen einzeln starten und/oder stoppen.

Bei der Darstellung im Menübaum kennzeichnet die Farbe des Listenpunkts den Status des Trace-Profiles (grün = Trace-Profil aktiviert, rot = Trace-Profil nicht aktiviert). Durch Auswahl von **Start/Stop Trace-Profil** kann ein nicht aktives Trace-Profil (roter Listenpunkt) aktiviert/gestartet und ein aktives Trace-Profil (grüner Listenpunkt) deaktiviert/gestoppt werden

Durch die Auswahl von **Trace-Profil anzeigen** können Sie die Details des gewünschten Trace-Profiles anzeigen: 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!

Trace-Profil	Anwendungsfall
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!
Xpressions 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 **Start/Stop Trace-Komponente** kann ein nicht aktives Trace-Profil (roter Listenpunkt) aktiviert/gestartet und ein aktives Trace-Profil (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.

24.9 TCP-Dump

Ein TCP-Dump dient zur Überwachung und Auswertung des Datenverkehrs in einer IP-Vernetzung.

Tipp: 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.
- Ermöglichen Sie autorisierten Servicetechnikern den Fernzugriff auf einen LAN-Trace.

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

24.10 RPCAP-Dämon

Ein RPCAP (Remote Packet Capture)-Dämon dient zur Überwachung und Auswertung des Datenverkehrs in einer IP-Vernetzung.

Tipp: 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)

24.11 Ereignisse

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.

Event Name	Send an SNMP Trap	Send an E-mail	Associated Trace Profile	Start Trace Profile	Stop Trace Profile
MSG_CAT_H323_REBOOT	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
MSG_CAT_HSA_REBOOT	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
MSG_GW_SUCCESSFULLY_STARTED	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
MSG_IP_LINK_FAILURE	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
MSG_IP_LINK2_FAILURE	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
MSG_IP_LINK3_FAILURE	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
MSG_WEBSERVER_MAJOR_ERROR	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
MSG_NEW_SW_AVAILABLE	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
MSG_ADMIN_REBOOT	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
MSG_SYSTEM_REBOOT	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
MSG_EXCEPTION_REBOOT	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
MSG_GW_OBJ_MEMORY_EXHAUSTED	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
ASSERTION_FAILED_EVENT	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
EXIT_REBOOT_EVENT	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
MSG_TLS_POOL_SIZE_EXCEEDED	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
MSG_OAM_RAM_THRESHOLD_REACHED	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
MSG_OAM_DMA_RAM_THRESHOLD_REACHED	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
MSG_OAM_THRESHOLD_REACHED	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
MSG_OAM_HIGH_TEMPERATURE_EXCEPTION	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
MSG_HACKER_ON_SNMP_PORT_TRAP	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
MSG_DVMOR_LAYER2_SERVICE_TRAP	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
H323_SNMP_TRAP	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
MSG_SSM_NUM_OF_CALL_LEGS_2BIG	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
MSG_SSM_SESSION_CREATION_FAILED	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
MSG_IPNCV_STARTUP_ERROR	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
MSG_IPNCV_STARTUP_SHUTDOWN	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
MSG_IPNCV_INTERNAL_ERROR	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
MSG_IPNCV_MEMORY_ERROR	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>

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.
- Kritisch: 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-Protokolle

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 Systemtelefonen (UP0 & HFA) angezeigt werden, siehe [Wie Sie die Ziele für die Alarm-Signalisierung festlegen](#). 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.

24.12 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.

Anmerkung: 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. Von 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.

Tipp: Eine Sicherung auf der Festplatte des Kommunikationssystems ist nicht möglich.

24.13 Card Manager

OpenScape Business wird mit bootfähigen Medien geliefert, die die Systemsoftware enthalten. Card Manager ist ein Tool für den Service-Support, um neue System-Software auf einer leeren SDHC-Karte, M.2 SATA SSD und UC Booster Card-Festplatte (HDD) zu erstellen. Dazu wird die Software des Kommunikationssystems als kompatible Image-Datei benötigt.

Die Software auf der SDHC-Karte, M.2 SATA SSD oder Festplatte ist eine Standard-System-Software ohne Kundendaten. Software-Updates oder das Sichern von Kundendaten sind damit nicht möglich. Es ist nur im Fall der SDHC-Karte möglich, eine Backup-Datei bei der Erstellung einzuschließen.

Card Manager kann als ISO-Image auf einer Linux-Boot-DVD und einem bootfähigen Linux-USB-Stick oder in einer virtuellen Umgebung gestartet werden.

Die Card Manager-Software ist über das Partner-Portal verfügbar.

Anwendungsfälle

- Vor Auslieferung des Systems soll die Software durch die aktuelle Software getauscht werden.
- Die Speichervorrichtung ist defekt und muss durch eine neue ersetzt 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.

24.14 Überwachung und Wartung der UC Suite

Das WBM bietet einem Administrator mit dem Profil **Expert** verschiedene Funktionen zur Überwachung und Wartung der UC Suite.

24.14.1 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**.

The screenshot shows the 'Server' configuration page with the 'Logging' tab selected. Under 'System Logging', the checkbox for 'Log Trace Messages (Verbose)' is unchecked. Under 'Client Logs', the 'Client Log Path' field is empty, 'Enable log upload' is unchecked, and 'Enable client logging' is checked. At the bottom, there are 'Save' and 'Reset' buttons.

Systemprotokolle

Folgendes Systemprotokoll kann aktiviert oder deaktiviert werden:

Systemprotokoll	Standardeinstellung
Trace-Meldungen protokollieren (ausführlich)	Nicht aktiviert

Die Ergebnisse des aktivierten Systemprotokolls werden 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/vs1/log` abgelegt.

Tipp: 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.

Tipp: Das Ablegen von Client Logs wird ausschließlich für die UC Suite Clients unterstützt, die mit Microsoft Windows Betriebssystemen 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** unter folgendem Pfad gespeichert: <Drive>:\Documents and Settings/<PC User Name>/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. Administratoren mit dem Profil **Advanced** können 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.

24.14.2 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.

Server

General Settings Live Record Logging **Notifications** Maintenance VoiceMail Contact Card Mapping

Email Notifications

- Enable email notifications of system errors
- Enable myPortal invitation email

Recipients: root@localhost

Conditions

- Send Critical Messages
- Send Crash Notifications

On error reporting, send the last 100 lines from the log file.

Save Reset

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
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

Systemfehler
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

24.14.3 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:

- Meldungen
- Anrufinformationen im Anrufjournal (Anrufhistorie)
- Mit myAgent aufgezeichnete Anrufe (Contact Center)
- Empfangene und gesendete Faxe und E-Mails für das Contact Center
- Log-Dateien

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 kritischen Füllstand erreicht hat.

The screenshot shows the 'Server' maintenance configuration interface. It includes tabs for 'General Settings', 'Live Record', 'Logging', 'Notifications', 'Maintenance' (selected), 'VoiceMail', and 'Contact Card Mapping'. The 'Maintenance' section contains several sub-sections: 'Begin system maintenance at 02:00' with a 'Clear Up Now' button; 'Message' retention settings (Keep inbox messages for 60 Day(s), Keep played / read messages for 30 Day(s), Keep saved messages for 365 Day(s), Keep deleted messages for 30 Day(s)); 'Fax' retention settings (Keep inbox faxes for 4 Day(s), Keep read faxes for 5 Day(s), Keep deleted faxes for 5 Day(s), Keep sent faxes for 5 Day(s)); and 'Calls Information Maintenance' (Keep call history for 365 Day(s), Close conversation after 5 Day(s)). 'Save' and 'Reset' buttons are located at the bottom of the page.

Für weitere Informationen zur **Wartung der Nachrichten** siehe [Sprachbox](#).

Für weitere Informationen zur **Wartung der Faxnachrichten** siehe [Faxbox](#).

Für weitere Informationen zur **Wartung der Anrufinformationen: Anrufliste**, siehe [Journal](#).

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.

Tipp: Die Aufbewahrungszeiten für die Wartung der Anrufinformationen sind unabhängig voneinander.

Contact-Center-Berichte basieren auf der Anrufliste. Wurde für die Anrufliste 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.

24.15 Überwachung der UC Smart

Den aktuellen Status der UC Smart kann ein Administrator mit dem Profil **Expert** über das WBM abrufen.

24.16 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 dem Höchstmaß an Sicherheit ist der Remote Service über RSP.servicelink zu bevorzugen. Weitere Informationen siehe [RSP.servicelink](#).

24.16.1 RSP.servicelink

Remotezugang mit der RSP.servicelink-Anschlussmöglichkeit (**R**emote **S**ervice **P**latform) bietet autorisierten Servicetechniker eines Remote Service Partners die Möglichkeit, das Kommunikationssystem inkl. der UC Booster Applikationen bequem und sicher aus der Ferne zu administrieren. Um RSP.servicelink zu konfigurieren, sind nur ein Internet-Anschluss, ein Webbrowser, die Partner ID und das Partner-Passwort des Remote Service Partners nötig. RSP.servicelink gewährleistet eine Breitbandverbindung mit hoher Sicherheit.

RSP.servicelink basiert auf der OpenVPN-Technologie. Es verwendet SSL/TSL-Protokoll und -Verschlüsselung und bietet mit einem zusätzlichen Client-Zertifikat die höchste Sicherheitsstufe. Der Begriff RSP.servicelink wird in der Dokumentation mit RSP abgekürzt.

In Verbindung mit OpenScape Business bietet RSP folgende wesentlichen Vorteile:

- Hohe 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 erforderlich, da dieser Port in der Firewall des Kunden in der Regel für gehende Internet-Anrufe schon geöffnet ist. Damit ist eine hohe Sicherheit für das Kundennetz garantiert.

Mit RSP behält der Administrator des Kommunikationssystems die Kontrolle über die Remote-Verbindung durch einfaches Ein- und Ausschalten des Zugangs. Bei RSP.servicelink wird automatisch auch 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 einen sogenannten RSP.servicelink. Bei der Aktivierung des Service Plugin müssen die Partner ID des Remote Service Partners und das Partner-Passwort eingegeben werden.

Jeder Remote Service Partner, der RSP.servicelink nutzt, hat eine eigene Partner ID.

Das RSP.servicelink-Plugin sollte deaktiviert und dann wieder aktiviert werden, wenn ein Software-Update durchgeführt wird.

- Zukunftssicherheit

RSP ist die Basis für zukünftige Services ("value-added" Services), wie zum Beispiel Automatisierung von Backups, Reporting und Monitoring.

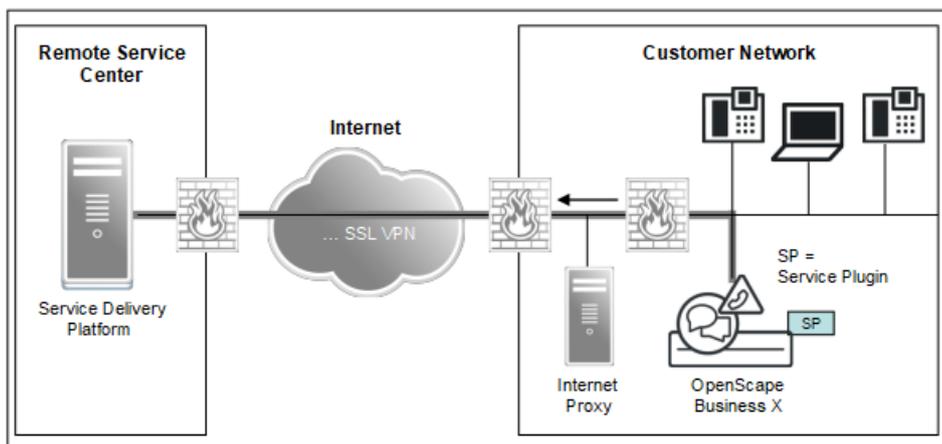


Abbildung 15: RSP - Übersicht für OpenScape Business X

RSP unterstützt die Web Services Standards, inklusive Hypertext Transfer Protocol Secure (HTTPS), 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 abgesichert.

Service-Plugins

Das RSP.servicelink-Plugin kann separat aktiviert oder deaktiviert werden.

Ein Zurücksetzen des RSP.servicelink-Plugins ist zum Beispiel nach dem Austausch des Mainboards erforderlich. Durch das Zurücksetzen des Service-Plugin wird die gesamte RSP-Konfiguration gelöscht und das Plugin deaktiviert.

Anmerkung: Wenn das System sich nicht im DTAG-Modus befindet und das RSP.servicelink-Plugin aktiviert ist, können die Proxykonfigurationseinstellungen nicht

geändert werden. Die Schaltfläche **Registrierung / Konfiguration ist deaktiviert**.

Wenn im DTAG-Modus das RSP.servicelink-Plugin aktiviert ist, wird bei einem Klick auf die Schaltfläche Registrierung / Konfiguration direkt die Seite Proxy-Einstellungen mit den Schaltflächen Abbrechen/Beenden aufgerufen. Dies ist auch vom Remote-Server aus möglich.

Geräteverwaltung (Managed Device)

Bei Kommunikationssystemen ohne UC Booster kann durch entsprechende Konfiguration auf SIRA-Seite der Fernzugriff für weitere Geräte (zum Beispiel Xpressions Compact) im Kunden-LAN ermöglicht werden. IP-Telefone können auf SIRA-Seite mit der Funktion "Verwaltete Geräte" konfiguriert werden.

Tipp: Der Fernzugriff auf andere im Kunden-LAN befindliche Kommunikationssysteme OpenScape Business ist nicht möglich. Jede OpenScape Business muss für den Fernzugriff konfiguriert werden.

Aktivierung/Deaktivierung

Es bestehen folgende Möglichkeiten zur Aktivierung/Deaktivierung der Service-Plugins:

- über Wizard **Aktivierung / Deaktivierung**

Für die RSP Service-Plugins 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**.

Sicherung und Wiederherstellung

Die RSP-Anmeldeinformationen werden im Backup-Set des Systems gespeichert.

Wenn ein neues OpenScape Business System durch Klonen oder durch Datenwiederherstellung (Migration) eingerichtet wird und auf dem ursprünglichen System ein RSP-Zugriff konfiguriert war, muss sichergestellt werden, dass auf dem geklonten oder wiederhergestellten System eine andere RSP-Konfiguration aktiv ist.

Sie müssen das RSP deaktivieren oder deinstallieren, bevor Sie das ursprüngliche System klonen oder sichern.

Wenn ein Zertifikat für die Verbindung zu RSP in mehr als einem System verwendet wird, wird das Zertifikat widerrufen und keines der OpenScape-Systeme kann eine Verbindung zum RSP-Dienst herstellen.

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.

Anmerkung: Wenn das System sich während des Systemstarts im DTAG-Modus befindet und ohne installiertes und konfiguriertes RSP.serviceplugin Zugang zum Internet hat, wird das RSP.serviceplugin mittels Skript automatisch mit der Partner-ID und dem Kennwort für DTAG (Gerätename entspricht der MAC-Adresse des Systems) installiert, konfiguriert und aktiviert. Außerdem wird das Skript regelmäßig alle 10 Minuten aufgerufen (z.B. für den Fall, dass nach der anfänglichen Systeminstallation kein Internetzugang verfügbar ist). Falls der Benutzer das Skript manuell deaktiviert hat, wird es vom RSP.serviceplugin nicht automatisch aktiviert.

24.16.2 Remote-Zugang

Durch den Remote-Zugang kann autorisierten Servicetechnikern über eine 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 besteht folgende Zugriffsmöglichkeit:

Remote-Zugang über Internet-Verbindung

Tipp: 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.

Anmerkung: Um nicht autorisierte Zugriffe auf das Kommunikationssystem zu vermeiden, ist der Remote-Zugang nach Beendigung der Fernadministration wieder auszuschalten.

24.16.3 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 unter http://apps.gdms.com:8081/techdoc/search_en.htm.

Auch das Servicetool Manager E bietet Online-Benutzer für die Fernsteuerung, -prüfung und -überwachung von OpenStage-Telefonen.

Anmerkung: Die vom Online-Benutzer genannte Gateway-IP-Adresse ist dieselbe wie die System-IP-Adresse. Die Gateway-IP-Adresse ist nicht die IP-Adresse der Standard-Route.

25 Migration

OpenScape Business V1, V2 Systeme und HiPath 3000 Systeme können auf OpenScape Business V3 migriert/aktualisiert werden.

Die folgenden Migrations-/Aktualisierungsszenarien werden von der OpenScape Business V3 Software unterstützt.

Anmerkung: Es ist wichtig, aktive Unify Phone-Benutzer z. B. vor Systemmigrationen zu löschen, um kritische Diskrepanzen zwischen der OpenScape Business-Datenbank und der Cloud-Datenbank zu vermeiden. Weitere Informationen finden Sie im Unify Experts Wiki unter: [Unify Phone Whitepaper](#)

OpenScape Business X System inklusive UC Booster Card oder Booster Server

- Software-Aktualisierung von OpenScape Business X V2 auf V3 mit „V2-Mainboard“
- Hardware-/Software-Migration von OpenScape Business X V2 auf V3 mit „V3-Mainboard“
- Hardware-/Software-Migration von OpenScape Business X V1 auf V3 mit „V3-Mainboard“
- Hardware-/Software-Migration von OpenScape Business X V3 mit „V2-Mainboard“ auf V3 mit „V3-Mainboard“

OpenScape Business S System

- Software-Aktualisierung von OpenScape Business S V2 auf V3

OpenScape Business Netzwerk

- Software-Aktualisierung von OpenScape Business Netzwerk von V2 auf V3

HiPath 3000 inklusive OpenScape Office HX

- Hardware-Migration HiPath 3000 inklusive OpenScape Office HX

HiPath 500

- Hardware-Migration HiPath 500 auf OpenScape Business X1 V3

Je nach Quellsystem können vorhandene Lizenzen ganz oder teilweise übertragen werden. Gleiches gilt für die weitere Verwendung von Peripheriemodulen und angeschlossenen Endgeräten.

Der bestehende Software-Support für OpenScape Business Systeme bleibt auch nach der Migration unverändert.

Sie können den Migrations-/Aktualisierungsaufwand für die weitere Nutzung vorhandener Lizenzen im Vergleich zu einer „Offline“-Lizenzübertragung verringern, wenn Sie das OpenScape Business System mit dem zentralen Unify-Lizenzserver verbinden und die Funktion **CLS Connect** nutzen.

In diesem Abschnitt werden die folgenden Begriffe verwendet:

Migration

Software-Aktualisierung für OpenScape Business X Systeme

Migration	bei Hardware- und Softwareänderungen
Upgrade	bei reinen Softwareänderungen
V2-Mainboard	Bezeichnung für die mit OpenScape Business eingeführte Mainboard-Familie.
V3-Mainboard	Bezeichnung für die mit der Software V3 eingeführte Mainboard-Familie.

Anmerkung: Wenn ein OpenScape Office V3 MX/LX System durch ein OpenScape Business System ersetzt werden soll, muss letzteres als neues System bestellt werden.

25.1 Software-Aktualisierung für OpenScape Business X Systeme

Die Software-Aktualisierung von OpenScape Business X Systemen beinhaltet im Wesentlichen den Ersatz einiger SW-Komponenten.

Vor der Aktualisierung eines OpenScape Business X Systems müssen Sie die aktuelle Systemkonfiguration und ggf. die zu ersetzenden Hardware-/Software- und Lizenzkomponenten bestimmen.

Tabelle 31: OpenScape Business X Software-Aktualisierung - Hardware-/Software-Checkliste

Komponenten	Ersetzt durch
Hardwarekomponenten	
Xpressions Compact Card	Smart VM oder UC Suite Voicemail
Softwarekomponenten	
V2 System-Software auf SDHC-Karte	V3 System-Software (Image vom Software Download Server)
VPN auf WAN im System beendet	VPN in externem Router beendet
XMPP	Keine Follow-on-Lösung
myPortal Smart	myPortal @work
Lizenzkomponenten	
Lizenzen in Lizenzdatei	Übertragung der Lizenzen in eine neue Lizenzdatei

25.1.1 Software-Aktualisierung von OpenScape Business X V2 auf OpenScape Business X V3

Wenn Sie eine SW-Aktualisierung des OpenScape Business X-Modells von Softwareversion V2 auf V3 vornehmen, wird nur die Systemsoftware ersetzt - das V2-Mainboard und alle vorhandenen UC Booster Cards oder Booster Server bleiben erhalten. Bestehende Lizenzen und die Kundenkonfiguration bleiben erhalten. Der bestehende Software-Support wird nach der Migration unverändert fortgeführt.

Falls dieser nicht bereits vorhanden ist, müssen Sie vor der Software-Aktualisierung von Version V2 auf V3 im System einen permanenten Zugang zum Unify-Lizenzserver einrichten (über das Internet) und die Funktion **CLS Connect** aktivieren. Das vereinfacht die Lizenzübertragung und verkürzt erheblich die Migrationszeit.

Voraussetzungen

Für die SW-Aktualisierung und die Übertragung der bestehenden Kundenkonfiguration muss das System mit der vor der Aktualisierung zuletzt veröffentlichten SW-Version V2R7 betrieben werden. Aktualisieren Sie ggf. das System auf die neueste SW-Version. Dazu muss das System über einen gültigen Software-Support-Status verfügen.

Für die System-SW-Aktualisierung von V2 auf V3 ist je nachdem, ob CLS Connect verwendet wird oder nicht, Folgendes erforderlich:

- OpenScape Business V3 SW Upgrade-Lizenz (nur wenn **CLS Connect** nicht verwendet wird)

Bedingungen und Einschränkungen für funktionale Grenzen

Sie können im Verlauf der Migration bestehende Lizenzen vom vorhandenen V2-Mainboard vollständig auf das V3 Mainboard übertragen. Die Lizenzübertragung ohne Aktivierung der Funktion CLS Connect erfordert die Lizenz „SW Upgrade“ und eine viel komplexere Handhabung und mehr Zeitaufwand als die Verwendung der Funktion CLS Connect.

Die Kundenkonfiguration und die Kundendaten werden beim SW-Aktualisierungsprozess von SW-Version V2 auf V3 automatisch übertragen.

Die wichtigsten technischen Schritte der SW-Aktualisierung werden in den folgenden Kapiteln beschrieben. Um die bestehenden Lizenzen beizubehalten, wird folgende Unterscheidung in der Handhabung gemacht:

- SW-Aktualisierung für permanente Lizenzierung mit und ohne CLS Connect
- SW-Aktualisierung mit PayGo-Lizenzierung

25.1.2 Software-Aktualisierung von OpenScape Business X V1 auf V2

Die Aktualisierung von OpenScape Business X Systemen mit SW-Version V1 auf SW-Version V2 besteht technisch gesehen aus der SW-Aktualisierung von SW-Version 1R3.3 auf Version 2R7.x und einer Lizenzmigration von V1-Lizenzen auf V2-Lizenzen. Die SW muss immer auf die zuletzt veröffentlichte SW-Version V2R7 aktualisiert werden, da sonst das System danach nicht nach SW-Version 3 migriert werden kann.

Nach der SW-Aktualisierung kann die vorhandene OpenScape Business Hardware vollständig genutzt werden. Für vorhandene UC Booster Server ist ebenfalls eine Software-Aktualisierung auf V2 erforderlich.

Für die Lizenzmigration von V1-Lizenzen auf V2-Lizenzen ist eine entsprechende Upgrade-Lizenz erforderlich.

Voraussetzungen

Für alle installierten OpenScape Business V1-Systeme mit einer zum Zeitpunkt der Veröffentlichung von V2 gültigen SW Assurance wurde von Unify automatisch eine permanente System-Upgrade-Lizenz auf V2 auf des Endkundenkonto am CLS gebucht (keine separate Bestellung erforderlich). Aktivieren Sie diese Lizenz am zentralen Lizenzserver (CLS), um bestehende V1-Lizenzen nach V2 zu migrieren.

Wenn die Lizenzen auf dem CLS von Version V1 nach Version V2 migriert wurden, ist der SW-Support für das OpenScape Business V2 System abgelaufen. Um für das System für die spätere Migration nach V3 wieder Software-Support zu erhalten, importieren Sie eine Wiederaufnahmelizenz und ggf. zusätzliche SW-Support-Lizenzen.

Bedingungen und Einschränkungen für funktionale Grenzen

Wenn das System von OpenScape Business V1 auf OpenScape Business V2 aktualisiert wird, ist eine ITSP-Aktivierung/Deaktivierung im Internet-Telefonie-Wizard erst dann möglich, wenn ein LCR-Reset durchgeführt wurde. Bereits in OpenScape Business V1 konfigurierte ITSPs funktionieren weiterhin in OpenScape Business V2 auch ohne LCR-Reset. Der bereits aktivierte ITSP kann bearbeitet jedoch nicht deaktiviert werden. Um im Wizard eine Änderung an der Aktivierung/Deaktivierung vorzunehmen, ist ein LCR-Reset erforderlich. Dies soll die nötigen Änderungen für die Erhöhung der ITSPs von 4 auf 8 widerspiegeln. Gehen Sie für das LCR-Reset zu **Experten-Modus > LCR > LCR-Flags** und klicken Sie auf das Flag **LCR-Daten zurücksetzen**.

Während der SW-Aktualisierung von OpenScape Business V1 zu OpenScape Business V2 wird der Web-Server-Prozess vom Mainboard (OCC) auf die Booster-Karte (OCAB) umgestellt, sofern verfügbar. Überprüfen Sie nach der Migration, ob die folgenden Anwendungen die korrekte IP-Adresse (IP-Adr des OCAB) verwenden: myPortal Smart, myPortal to go, myPortal OpenStage, OpenScape Business

Attendant, OpenScape TAPI120 im UC Smart Modus, Application Launcher, 3rd Party Web Service Application.

Aktualisierung Schritt für Schritt

Führen Sie für eine SW-Aktualisierung eines OpenScape Business X V1 Systems auf V2 die folgenden Migrationsschritte der Reihe nach durch:

1) OpenScape Business V1 Software aktualisieren

Aktualisieren Sie mithilfe des WBM die OpenScape Business V1 Software auf die Version V1 R3.3 (siehe [Update des Kommunikationssystems](#) auf Seite 711).

2) OpenScape Business V2 Lizenzdatei laden

Laden Sie die OpenScape Business V2 Lizenzdatei in das OpenScape Business V1 System und aktivieren Sie die Lizenzen (siehe [Lizenzaktivierung \(Standalone\)](#) auf Seite 167).

3) Aktuelle OS Biz V2 Software laden

Laden Sie mit Hilfe des WBM die aktuelle OpenScape Business V2 Software in das Kommunikationssystem. Die V1-Daten werden dabei automatisch in V2-Daten konvertiert (siehe [Update des Kommunikationssystems](#) auf Seite 711).

4) Datensicherung durchführen

Sichern Sie Ihre V2-Daten (siehe [Sofortiges Sichern](#) auf Seite 707).

25.2 Software-Aktualisierung von UC Booster Server auf OpenScape Business X V3

Die SW-Aktualisierung von einem UC Booster Server V2 auf V3 kann in einem Schritt durchgeführt werden.

Eine SW-Aktualisierung von einem UC Booster Server V1 auf Version V3 muss in zwei Schritten erfolgen. Aktualisieren Sie zuerst von V1 auf V2R7, dann von V2R7 auf V3.

25.2.1 Wie Sie UC Business Booster Server V2 auf V3 aktualisieren

Die SW-Aktualisierung des UC Booster Server von V2 auf V3 ist nur für OpenScape Business X Systeme mit einem V2-Mainboard notwendig. OpenScape Business X Systeme mit V3-Mainboards erfordern keinen UC Booster Server mehr. In diesem Fall wird die SW-Version V2.7 auf dem UC Booster Server benötigt, um die Kundenkonfiguration und die Lizenzen auf das V3-Mainboard zu migrieren.

Voraussetzungen

- Das Linux Betriebssystem muss überprüft und ggf. aktualisiert werden (siehe *Technical Release note OpenScape Business V3 system SW*)

- UC Booster Server wird vor der Aktualisierung mit der zuletzt veröffentlichten SW-Version V2R7 betrieben. Aktualisieren Sie ggf. das System auf die neueste SW-Version.
- Aktualisieren Sie zuerst das OpenScape Business X System, mit dem der UC Booster Server verbunden ist, auf SW-Version V3 einschließlich Lizenzierung gemäß der Beschreibung in [Software-Aktualisierung von OpenScape Business X V2 auf OpenScape Business X V3](#) auf Seite 763
- UC Booster Server SW-Image V3

Bestimmen Sie vor der SW-Aktualisierung des UC Booster Server die aktuelle Systemkonfiguration und ggf. die zu ersetzenden HW-/SW- und Lizenzkomponenten.

Tabelle 32: Migration von OpenScape Business S - HW-/SW-Checkliste

Komponenten	Ersetzt durch
Hardwarekomponenten	
Server-PC	Wiederverwendung ist möglich. Die HW-Anforderungen müssen für OpenScape Business S-Erweiterungen geprüft werden. ⁹
Softwarekomponenten	
Betriebssystem SLES 12	Wiederverwendung ist möglich. Schließlich ist eine Aktualisierung auf das neueste Service Pack erforderlich ¹⁰
XMPP	Keine Follow-on-Lösung
myPortal Smart	myPortal @work
Lizenzkomponenten	

⁹ Die bestehende PC-HW kann verwendet werden, wenn das UC Booster Server System nach der SW-Aktualisierung unverändert bleibt. Wenn nach der SW-Aktualisierung Erweiterungen geplant sind, müssen die Hardwareanforderungen ggf. gemäß den Spezifikationen in *OpenScape Business S Installationsanleitung, Kapitel Voraussetzungen* angepasst werden.

¹⁰ Das auf dem Server-PC installierte SLES-Betriebssystem kann im Fall einer SW-Aktualisierung des UC Booster Server angepasst werden. Allerdings sollte vor der SW-Aktualisierung auf das letzte veröffentlichte Service Pack aktualisiert werden.

Wenn Novell den SW-Support für die verwendete SLES-Version eingestellt hat, muss der Kunde informiert und ggf. eine SLES-Aktualisierung verkauft werden.

Die SLES-Aktualisierung muss möglicherweise in mehreren Schritten durchgeführt werden, um bestehende Installationen von OpenScape Business S gemeinsam mit der Kundenkonfiguration und den Kundendaten zu übernehmen. Ein vorhandener SLES Update Key bleibt mit einer SLES-Aktualisierung gültig. Seine Registrierung bei Novell muss jedoch ggf. vor der SLES-Aktualisierung aufgehoben werden, bevor er für das neue System erneut registriert wird.

Komponenten	Ersetzt durch
Lizenzen in Lizenzdatei (ist Teil der OpenScape Business X Lizenzdatei)	Übertragung der Lizenzen in eine neue Lizenzdatei
CSTA-Applikation (über UC Booster Card / Server)	CSTA-Lizenz für den Anschluss externer Lösungen (nicht erforderlich für UC Suite, TAPI 170 und TAPI 120)

Im Folgenden wird die SW-Aktualisierung von OpenScape Business unter Beibehaltung des SLES-Betriebssystems beschrieben.

Schritt für Schritt

1. Aktualisierung von OpenScape Business X System auf V3.
Siehe [Software-Aktualisierung von OpenScape Business X V2 auf OpenScape Business X V3](#) auf Seite 763 für Details.
2. Aktualisierung der UC Booster Server SW auf V3
Verwenden Sie die Aktualisierungsfunktion im OpenScape Business Assistant des UC Booster Server zur Aktualisierung der V2R7-SW auf die Version V3 (siehe [Update des Kommunikationssystems](#) auf Seite 711).
3. Führen Sie nach der SW-Aktualisierung eine Datensicherung durch
Sichern Sie Ihre V3-Daten (siehe [Sofortiges Sichern](#) auf Seite 707)

25.2.2 Wie Sie UC Business Booster Server V1 auf V2 aktualisieren

Um einen OpenScape Business V1 UC Booster Server auf einen OpenScape Business V2 UC Booster Server zu aktualisieren, führen Sie die nachstehend beschriebenen Migrationsschritte durch.

Voraussetzungen

Prüfen Sie vor der Migration, ob die Hard- und Softwareeigenschaften des Linux-Servers für UC Booster Server V2 ausreichend sind. Eine Aktualisierung des Linux Servers reicht aus (z. B. mehr Arbeitsspeicher). Das SLES 64-Bit-Linux-Betriebssystem für UC Booster Server V2 ist eine Voraussetzung. Wählen Sie für einen weiteren Aktualisierungsschritt auf UC Booster Server V3 die für V3 veröffentlichte SLES 64-Bit-Version.

Wird ein neuer Linux Server benötigt, installieren Sie nach der Linux-Installation die OpenScape Business V1 S Kommunikationssoftware. Eine V1-Datensicherung kann dann übertragen werden und Sie können anschließend mit der Migration fortfahren.

Schritt für Schritt

1. Aktualisierung von OpenScape Business X1 und UC Booster Server auf die V1R3.3 Software

Migration

Hardware/Software-Migration von OpenScape Business X Systemen auf V3

- Aktualisieren Sie mithilfe des WBM die OpenScape Business V1 Software auf die Version V1 R3.3 oder höher (siehe [Update des Kommunikationssystems](#) auf Seite 711).
2. Aktualisierung von OpenScape Business X System auf V2
Siehe [Software-Aktualisierung von OpenScape Business X V1 auf V2](#) auf Seite 764 für Details.
 3. Aktualisierung der UC Booster Server SW auf V2
Verwenden Sie die Aktualisierungsfunktion im OpenScape Business Assistant des UC Booster Server zur Aktualisierung der V1-SW auf die Version V2 (siehe [Update des Kommunikationssystems](#) auf Seite 711).
 4. Führen Sie nach der SW-Aktualisierung eine Datensicherung durch
Sichern Sie Ihre V3-Daten (siehe [Sofortiges Sichern](#) auf Seite 707)

25.3 Hardware/Software-Migration von OpenScape Business X Systemen auf V3

Bei der Migration von OpenScape Business X Systemen werden HW-, SW- und Lizenzkomponenten ausgetauscht.

Bestimmen Sie vor der Migration eines Business X Systems die aktuelle Systemkonfiguration und die zu ersetzenden HW-, SW-Lizenzkomponenten.

Anmerkung: Die OCCLA-Platine mit V3-System kann bis zu 60 (+16) MEB-Kanäle aufnehmen. Bei der Migration auf die neue Platine wird die bestehende OCC-Konfiguration wiederhergestellt. Wenn Sie die Vorteile der zusätzlichen MEB-Kanäle nutzen möchten, sollten Sie Ihr System mit Hilfe der entsprechenden Assistenten/WBM-Seiten neu konfigurieren.

Module, die in Steckplatz 10 von OpenScape Business X5 Wandsystemen vorhanden sind, können nicht in Verbindung mit V3-Mainboards betrieben werden. Diese Module müssen durch Nachfolgemodule/-lösungen ersetzt werden.

Tabelle 33: Migration von OpenScape Business X - HW-/SW-Checkliste

Komponente	Ersetzt durch
Hardwarekomponenten	
Vorhandenes „V2-Mainboard“	V3-Mainboard (einfache oder erweitert, je nach Konfiguration)
UC Booster Card / Server (mit UC Suite)	Zusätzliche M.2 SSD
CMA-Modul	CMAe-Modul

Komponente	Ersetzt durch
EXMR-Modul für externe Ansagegeräte	V3-Mainboard (Audio-In-Buchse auf der Vorderseite)
S0-Schnittstellena auf dem V2-Mainboard	S0-Anschluss der S0-Peripheriekarte
Xpressions Compact Card	Smart VM oder UC Suite Voicemail
X5W-Karten für Steckplatz 10 <ul style="list-style-type: none"> • SLCN16 • SLA16N • SLA24N 	Ersetzt durch: <ul style="list-style-type: none"> • Schnurlose Direktverbindung • SLAV16 • SLAV16 + SLAV8
Optipoint 500 Telefone	OpenScape Deskphone CP Telefone
Optipoint 400 Telefone	
Softwarekomponenten	
V2 System-SW auf SDHC-Karte	V3 System-SW (Image vom Software Download Server)
VPN auf WAN im System beendet	VPN in externem Router beendet
XMPP	Keine Follow-on-Lösung
myPortal Smart	myPortal @work
Lizenzkomponenten	
Lizenzen in Lizenzdatei	Übertragung der Lizenzen in eine neue Lizenzdatei
Externe CSTA-Anwendungen (bisher lizenzfrei, da an UC Booster-Karte / Server HW angeschlossen)	Separate CSTA-Lizenz für den Anschluss externer Lösungen (nicht erforderlich für UC Suite, TAPI 170 und TAPI 120)

25.3.1 Migration von OpenScape Business X V2 auf OpenScape Business X V3

Bei der Migration eines OpenScape Business X-Modells von V2 auf V3 werden das Mainboard und die Systemsoftware ersetzt. Bestehende Lizenzen und die Kundenkonfiguration können übertragen werden. Der bestehende Software-Support wird nach der Migration unverändert fortgeführt.

Vor der Migration müssen Sie im System einen permanenten Zugang zum Unify-Lizenzserver konfigurieren (über das Internet) und die Funktion „CLS Connect“ aktivieren. Das vereinfacht die Lizenzübertragung und verkürzt erheblich die Migrationszeit. Der Kunde muss über den erforderlichen Zugang vom OpenScape Business System zum CLS informiert werden.

Voraussetzungen

Das System wird vor der Aktualisierung mit der zuletzt veröffentlichten SW-Version V2R7 betrieben. Aktualisieren Sie ggf.

das System auf die neueste SW-Version. Dazu muss das System über einen gültigen Software-Support-Status verfügen.

Für die Migration von V2 auf V3 ist Folgendes erforderlich, je nachdem, ob CLS Connect, UC Suite oder externe CSTA-Applikationen verwendet werden folgenden Artikel wurden:

- V3-Mainboard
- V3 SW auf M.2 SATA SSD-Datenspeicher
- M.2 SSD 256 GB Massenspeicher (optional mit Applikation UC Suite)
- OpenScape Business V3 HW-Migrationslizenz (falls CLS Connect nicht verwendet wird)
- OpenScape Business CSTA-Lizenz (optional)

Bedingungen und Einschränkungen für funktionale Grenzen

Während der Migration können bestehende Lizenzen vom vorhandenen V2-Mainboard vollständig auf das V3 Mainboard übertragen werden. Die Lizenzübertragung ohne Aktivierung der Funktion CLS Connect erfordert die Lizenz „HW-Migration“ und eine viel komplexere Handhabung und mehr Zeitaufwand als die Verwendung der Funktion CLS Connect.

Die Kundenkonfiguration und die Kundendaten werden über einen Sicherungs-/Wiederherstellungsprozess von SW-Version V2 auf V3 migriert.

Die wichtigsten technischen Schritte der Migration werden in den folgenden Abschnitten beschrieben. Um die bestehenden Lizenzen beizubehalten, wird folgende Unterscheidung in der Handhabung gemacht:

- SW-Aktualisierung für permanente Lizenzierung mit und ohne CLS Connect
- SW-Aktualisierung mit PayGo-Lizenzierung

Anmerkung: Bei der Migration von V2-Mainboard auf V3-Mainboard werden die zusätzlichen EVM-Ports nicht zusätzlich in den SmartVM-Sammelanschluss aufgenommen. Dies erfordert eine manuelle Konfiguration, in deren Verlauf man auch die COS-Einschränkung vornehmen sollte.

25.3.1.1 Wie Sie permanent lizenzierte Systeme mit CLS Connect auf V3 migrieren

Führen Sie folgende Migrationsschritte der Reihe nach durch:

Schritt für Schritt

- 1.** Bereiten Sie das OpenScape Business System vor
 - a) Aktualisieren Sie das vorhandene System auf SW-Version V2R7

- b) Richten Sie im System einen Zugang zum zentralen Lizenzserver (Central License Server, CLS) ein und testen Sie die Verbindung
- c) Aktivieren Sie CLS Connect im System
- 2. Generieren Sie die Lizenzdatei auf dem zentralen Lizenzserver (CLS)
 - a) Übertragen Sie die bestehenden Lizenzen von der MAC-Adresse des V2-Mainboards mithilfe der Funktion **Neu generieren** auf die MAC-Adresse des V3-Mainboards
 - b) Generieren Sie eine neue Lizenzdatei für die MAC-Adresse auf dem V3-Mainboard
- 3. Sichern Sie die V2-Systemkonfiguration und die Kundendaten.
- 4. Tauschen Sie die Mainboards
 - a) Fahren Sie das System herunter und schalten Sie alle Versorgungsspannungen aus
 - b) Verwenden Sie V3-Datenträger und ggf. optionale Massenspeicher auf dem V3-Mainboard
 - c) Entfernen Sie die OCCB Voice Channel Booster Karte vom V2-Mainboard und stecken Sie sie in das V3-Mainboard ein.
 - d) Ersetzen Sie das V2-Mainboard im System durch das V3-Mainboard
 - e) Schalten Sie die Versorgungsspannungen wieder ein
Das System startet automatisch.
- 5. Stellen Sie nach dem Hochfahren die grundlegenden Systemparameter in WBM ein
 - a) Stellen Sie Systemdatum und -uhrzeit ein
 - b) Stellen Sie das Anwendungspaket ein
UC Smart für System ohne UC oder mit UC Smart
UC Suite für Systeme mit UC Suite
- 6. Stellen Sie die Systemkonfiguration wieder her
 - a) Stellen Sie die Sicherung mithilfe der Wiederherstellungsfunktion wieder her
 - b) Importieren Sie die neu erstellte Lizenzdatei

25.3.1.2 Wie Sie permanent lizenzierte Systeme ohne CLS Connect auf V3 migrieren

Führen Sie folgende Migrationsschritte der Reihe nach durch:

Schritt für Schritt

1. Bereiten Sie das OpenScape Business System vor
 - a) Aktualisieren Sie das vorhandene System auf SW-Version V2R7
2. Erstellen Sie auf dem zentralen Lizenzserver (CLS) die „Migrations-Lizenzdatei“ für das V2-System
 - a) Aktivieren Sie die „HW-Migrationslizenz“ für das vorhandene System

- b) Generieren Sie eine neue Lizenzdatei für die MAC-Adresse des V2-Mainboards.
Geben Sie dazu die MAC-Adresse des V3-Mainboards ein.
- c) Laden Sie die Lizenzdatei vom CLS herunter
- 3.** Importieren Sie die Lizenzdatei in das OpenScape Business V2-System
- 4.** Notieren Sie den **Bestätigungscode**, der im OpenScape Business Assistant angezeigt wird
- 5.** Generieren Sie auf dem zentralen Lizenzserver (CLS) eine neue Lizenzdatei für das V3-Mainboard
 - a) Erstellen Sie auf dem CLS eine neue Lizenzdatei für die MAC-Adresse des V3-Mainboards, indem Sie die MAC-Adresse des V2-Mainboards mit dem zuvor notierten Bestätigungscode erneut generieren
 - b) Suchen Sie auf dem CLS das OpenScape Business System mit der MAC-Adresse der V3-Mainboards.
 - c) Entsperren Sie das OpenScape Business System, indem Sie den Bestätigungscode eingeben und aktivieren
 - d) Generieren Sie die Lizenzdatei erneut
 - e) Laden Sie die neu generierte Lizenz vom CLS herunter
- 6.** Sichern Sie die V2-Systemkonfiguration und die Kundendaten.
- 7.** Tauschen Sie die Mainboards
 - a) Fahren Sie das System herunter und schalten Sie alle Versorgungsspannungen aus
 - a)** Verwenden Sie V3-Datenträger und ggf. optionale Massenspeicher auf dem V3-Mainboard
 - b)** Entfernen Sie die OCCB Voice Channel Booster Karte vom V2-Mainboard und stecken Sie sie in das V3-Mainboard ein.
 - c)** Ersetzen Sie das V2-Mainboard im System durch das V3-Mainboard
 - b) Schalten Sie die Versorgungsspannungen wieder ein
Das System startet automatisch.
- 8.** Stellen Sie nach dem Hochfahren die grundlegenden Systemparameter in WBM ein
 - a) Stellen Sie Systemdatum und -uhrzeit ein
 - b) Stellen Sie das Anwendungspaket ein
UC Smart für System ohne UC oder mit UC Smart
UC Suite für Systeme mit UC Suite
- 9.** Stellen Sie die Systemkonfiguration wieder her
 - a) Stellen Sie die Sicherung mithilfe der Wiederherstellungsfunktion wieder her
- 10.** Importieren Sie nach dem Hochfahren des Systems manuell die neue Lizenzdatei in das V3-System

25.3.1.3 Wie Sie PayGo-lizenzierte Systeme auf V3 migrieren

Führen Sie folgende Migrationsschritte der Reihe nach durch:

Schritt für Schritt

1. Bereiten Sie das OpenScape Business System vor
 - a) Aktualisieren Sie das vorhandene System auf SW-Version V2R7
2. Sichern Sie die V2-Systemkonfiguration und die Kundendaten.
3. Generieren Sie die Lizenzdatei auf dem zentralen Lizenzserver (CLS) neu
 - a) Generieren Sie erneut eine neue Lizenzdatei für die MAC-Adresse auf dem V3-Mainboard
Übertragen Sie die bestehenden Lizenzen von der MAC-Adresse des V2-Mainboards auf die MAC-Adresse des V3-Mainboards.
 - b) Laden Sie die neue Lizenzdatei vom CLS herunter
4. Tauschen Sie die Mainboards
 - a) Fahren Sie das System herunter und schalten Sie alle Versorgungsspannungen aus
 - b) Verwenden Sie V3-Datenträger und ggf. optionale Massenspeicher auf dem V3-Mainboard
 - c) Entfernen Sie die OCCB Voice Channel Booster Karte vom V2-Mainboard und stecken Sie sie in das V3-Mainboard ein.
 - d) Ersetzen Sie das V2-Mainboard im System durch das V3-Mainboard
 - e) Schalten Sie die Versorgungsspannungen wieder ein
Das System startet automatisch.
5. Stellen Sie nach dem Hochfahren die grundlegenden Systemparameter in WBM ein
 - a) Stellen Sie Systemdatum und -uhrzeit ein
 - b) Stellen Sie das Anwendungspaket ein
UC Smart für System ohne UC oder mit UC Smart
UC Suite für Systeme mit UC Suite
6. Stellen Sie die Systemkonfiguration wieder her
 - a) Stellen Sie die Sicherung mithilfe der Wiederherstellungsfunktion wieder her
7. Importieren Sie manuell die neue Lizenzdatei in das V3-System und aktivieren Sie die Lizenzdatei

25.3.2 Migration von OpenScape Business X V1 auf OpenScape Business X V3

Bei der Migration eines OpenScape Business X-Modells von V1 auf V3 werden das Mainboard und die Systemsoftware ersetzt.

Führen Sie die Migration in zwei Schritten durch.

- SW-Aktualisierung der SW-Version V1R3 auf die zuletzt veröffentlichte SW-Version V2R7.
- Migration des V2-Systems auf das V3-System

Mit diesem Verfahren können bestehende Lizenzen und die Kundenkonfiguration übernommen werden. Nach der Migration in [Schritt 2: Migration des V2-Systems auf das V3-System](#) auf Seite

Migration

OpenScape Business X V3 System von einem V2-Mainboard auf ein V3-Mainboard migrieren

774 muss sichergestellt werden, dass das System über SW-Support verfügt.

25.3.2.1 Schritt 1: Software-Aktualisierung von Version V1R3 auf zuletzt veröffentlichte Version V2R7

Die Aktualisierung von OpenScape Business X Systemen mit SW-Version V1R3.3 auf SW-Version V2 besteht technisch gesehen aus der SW-Aktualisierung von SW-Version 1R3.3 auf Version 2R7.x und einer Lizenzmigration von V1-Lizenzen auf V2-Lizenzen.

Sie müssen die Software immer auf die zuletzt veröffentlichte SW-Version V2R7 aktualisieren, da sonst das System danach nicht nach SW-Version 3 migriert werden kann.

Nach der SW-Aktualisierung kann die gesamte vorhandene OpenScape Business Hardware genutzt werden. Für vorhandene UC Booster Server ist ebenfalls eine Software-Aktualisierung auf V2 erforderlich.

Für die Lizenzmigration von V1-Lizenzen auf V2-Lizenzen ist eine entsprechende Upgrade-Lizenz erforderlich.

Für alle installierten OpenScape Business V1-Systeme mit einer zum Zeitpunkt der Veröffentlichung von V2 gültigen SW Assurance wurde von Unify automatisch eine permanente System-Upgrade-Lizenz auf V2 auf des Endkundenkonto am CLS gebucht (keine separate Bestellung erforderlich). Diese Lizenz muss am zentralen Lizenzserver (CLS) aktiviert werden, um bestehende V1-Lizenzen nach V2 zu migrieren.

Wenn die Lizenzen auf dem CLS von Version V1 nach Version V2 migriert wurden, ist der SW-Support für das OpenScape Business V2 System abgelaufen. Um für das System für die spätere Migration nach V3 wieder Software-Support zu erhalten, importieren Sie eine Wiederaufnahmelizenz und ggf. zusätzliche SW-Support-Lizenzen.

Die Schritte für eine SW-Aktualisierung von OpenScape Business X System von V1 auf V2 sind in [Software-Aktualisierung von OpenScape Business X V1 auf V2](#) auf Seite 764 beschrieben.

25.3.2.2 Schritt 2: Migration des V2-Systems auf das V3-System

Für die anschließende Migration des Systems von V2 auf V3 gelten die in [Migration von OpenScape Business X V2 auf OpenScape Business X V3](#) auf Seite 769 beschriebenen Verfahren. Für diesen Schritt benötigen Sie zusätzliche HW-/SW-Komponenten und möglicherweise auch Lizenzen.

25.4 OpenScape Business X V3 System von einem V2-Mainboard auf ein V3-Mainboard migrieren

In diesem Szenario wird das bestehende V2-Mainboard des OpenScape Business Systems und möglicherweise vorhandene UC

Booster HW mit einem V3-Mainboard ersetzt. Das System wurde zuvor auf die SW-Version V3 aktualisiert, z. B. im Zuge des SW-Supports.

Bestehende Lizenzen und die Kundenkonfiguration können übertragen werden. Der bestehende Software-Support wird nach der Migration unverändert fortgeführt.

Eine möglicherweise vorhandene UC Booster Card oder ein UC Booster Server sind in Verbindung mit dem V3-Mainboard nicht mehr notwendig. Zu diesem Zweck wird auf dem V3-Mainboard ein zusätzlicher Massenspeicher verwendet.

In [Tabelle 33: Migration von OpenScape Business X - HW-/SW-Checkliste](#) auf Seite 768 finden Sie Informationen, welche Komponenten durch die Verwendung des V3-Mainboards ersetzt oder ersatzlos gestrichen wurden. Eine CSTA-Lizenz ist für eine bestehende Verbindung zu externen CSTA-Applikationen erforderlich. Das gilt nicht für die Verbindung zu OpenScape TAPI 170 oder TAPI 120.

Voraussetzungen

Das System wird vor der Aktualisierung mit der zuletzt veröffentlichten SW-Version V2R7 betrieben. Aktualisieren Sie ggf. das System auf die neueste SW-Version. Dazu muss das System über einen gültigen Software-Support-Status verfügen.

Für die Migration ist Folgendes erforderlich, je nachdem, ob CLS Connect, UC Suite oder externe CSTA-Applikationen verwendet werden:

- V3-Mainboard
- V3 SW auf M.2 SATA SSD-Datenspeicher
- M2 SSD 256 GB Massenspeicher (optional mit Applikation UC Suite)
- OpenScape Business V3 HW-Migrationslizenz (optional)
- OpenScape Business CSTA-Lizenz (optional)

Bedingungen und Einschränkungen für funktionale Grenzen

Im Verlauf der Migration können bestehende Lizenzen vom vorhandenen V2-Mainboard vollständig auf das V3 Mainboard übertragen werden. Die Lizenzübertragung ohne Aktivierung der Funktion CLS Connect erfordert die Lizenz „HW-Migration“ und eine viel komplexere Handhabung und mehr Zeitaufwand als die Verwendung der Funktion CLS Connect.

Die Kundenkonfiguration und die Kundendaten werden über den Sicherungs-/Wiederherstellungsprozess übertragen.

Die wichtigsten technischen Schritte der Migration werden in den folgenden Abschnitten beschrieben. Um die bestehenden Lizenzen beizubehalten, wird folgende Unterscheidung in der Handhabung gemacht:

- SW-Aktualisierung für permanente Lizenzierung mit und ohne CLS Connect
- SW-Aktualisierung mit PayGo-Lizenzierung

Anmerkung: Bei der Migration von V2 Mainboard auf V3 Mainboard werden die zusätzlichen EVM-Ports nicht zusätzlich in den SmartVM-Sammelanschluss aufgenommen. Dies erfordert eine manuelle Konfiguration, in deren Verlauf man auch die COS-Einschränkung vornehmen sollte.

Die Konvertierung eines KDS in derselben Softwareversion in einen anderen Systemtyp wird von Manager E nicht unterstützt. Wenn Sie nur die KDS-Daten verwenden möchten, können Sie die folgenden Schritte versuchen:

- Führen Sie eine vollständige Migration von einem V2-Mainboard zu einem V3-Mainboard-System durch.
- Laden Sie das V3-Mainboard-System KDS mit Manager E herunter und speichern Sie es lokal.
- Laden Sie das V3-Mainboard-System neu.
- Laden Sie das zuvor gespeicherte V3-Mainboard-KDS in Ihr V3-Mainboard-System hoch.

Das V3-Mainboard-System verwendet die KDS-Datenbankkonfiguration und Sie können mit der manuellen UC-Konfiguration fortfahren.

Anmerkung: Die Migration des KDS des V2-Mainboard-Systems auf das V3-Mainboard-System wird nicht unterstützt, da die Datenbank des V2-Mainboards nicht mit der Datenbank des V3-Mainboards kompatibel ist.

25.4.1 Wie Sie permanent lizenzierte Systeme mit CLS Connect auf ein V3-Mainboard migrieren

Führen Sie folgende Migrationsschritte der Reihe nach durch:

Schritt für Schritt

1. Bereiten Sie das OpenScape Business System vor
 - a) Richten Sie im System einen Zugang zum zentralen Lizenzserver (Central License Server, CLS) ein und testen Sie die Verbindung
 - b) Aktivieren Sie CLS Connect im System
2. Generieren Sie die Lizenzdatei auf dem zentralen Lizenzserver (CLS)
 - a) Übertragen Sie die bestehenden Lizenzen von der MAC-Adresse des V2-Mainboards mithilfe der Funktion **Neu generieren** auf die MAC-Adresse des V3-Mainboards
 - b) Generieren Sie eine neue Lizenzdatei für die MAC-Adresse auf dem V3-Mainboard
3. Sichern Sie die V3-Systemkonfiguration und die Kundendaten.
4. Erstellen Sie ggf. eine Sicherung der Booster Server-Konfiguration.

5. Tauschen Sie die Mainboards
 - a) Fahren Sie das System herunter und schalten Sie alle Stromversorgungen aus
 - b) Verwenden Sie V3-Datenträger und ggf. optionale Massenspeicher auf dem V3-Mainboard
 - c) Entfernen Sie die OCCB Voice Channel Booster Karte vom V2-Mainboard und stecken Sie sie in das V3-Mainboard ein.
 - d) Ersetzen Sie das V2-Mainboard im System durch das V3-Mainboard
 - e) Schalten Sie die Versorgungsspannungen wieder ein
Das System startet automatisch.
6. Stellen Sie nach dem Hochfahren die grundlegenden Systemparameter in WBM ein
 - a) Stellen Sie Systemdatum und -uhrzeit ein
 - b) Stellen Sie das Anwendungspaket ein
UC Smart für System ohne UC oder mit UC Smart
UC Suite für Systeme mit UC Suite
7. Stellen Sie die Systemkonfiguration wieder her
 - a) Importieren Sie die neu erstellte Lizenzdatei
 - b) Stellen Sie mithilfe der Wiederherstellungsfunktion die Systemsicherung und ggf. die Booster Server-Sicherung wieder her

25.4.2 Wie Sie permanent lizenzierte Systeme ohne CLS Connect auf ein V3-Mainboard migrieren

Führen Sie folgende Migrationsschritte der Reihe nach durch:

Schritt für Schritt

1. Erstellen Sie auf dem zentralen Lizenzserver (CLS) die „Migrations-Lizenzdatei“ für das vorhandene V2-Mainboard
 - a) Aktivieren Sie die „HW-Migrationslizenz“ für das vorhandene System
 - b) Generieren Sie eine neue Lizenzdatei für die MAC-Adresse des V2-Mainboards
Dazu muss die MAC-Adresse des V3-Mainboards eingegeben werden.
 - c) Laden Sie die Lizenzdatei vom CLS herunter
2. Importieren Sie die Lizenzdatei in das OpenScape Business System mit V2-Mainboard.
3. Notieren Sie den **Bestätigungscode**, der im OpenScape Business Assistant angezeigt wird
4. Generieren Sie auf dem zentralen Lizenzserver (CLS) eine neue Lizenzdatei für das V3-Mainboard
 - a) Erstellen Sie auf dem CLS eine neue Lizenzdatei für die MAC-Adresse des V3-Mainboards, indem Sie die MAC-Adresse des V2-Mainboards mit dem zuvor notierten Bestätigungscode erneut generieren.

- a) Suchen Sie auf dem CLS das OpenScape Business System mit der MAC-Adresse der V3-Mainboards.
 - b) Entsperren Sie das OpenScape Business System, indem Sie den Bestätigungscode eingeben und aktivieren
 - c) Generieren Sie die Lizenzdatei erneut
- b) Laden Sie die neu generierte Lizenz vom CLS herunter.
5. Sichern Sie die Systemkonfiguration und die Kundendaten.
 6. Tauschen Sie die Mainboards
 - a) Fahren Sie das System herunter und schalten Sie alle Versorgungsspannungen aus
 - b) Verwenden Sie V3-Datenträger und ggf. optionale Massenspeicher auf dem V3-Mainboard
 - c) Entfernen Sie die OCCB Voice Channel Booster Karte vom V2-Mainboard und stecken Sie sie in das V3-Mainboard ein.
 - d) Ersetzen Sie das V2-Mainboard im System durch das V3-Mainboard
 - e) Schalten Sie die Versorgungsspannungen wieder ein
Das System startet automatisch.
 7. Stellen Sie nach dem Hochfahren die grundlegenden Systemparameter in WBM ein
 - a) Stellen Sie Systemdatum und -uhrzeit ein
 - b) Stellen Sie das Anwendungspaket ein
UC Smart für System ohne UC oder mit UC Smart
UC Suite für Systeme mit UC Suite
 8. Stellen Sie nach dem Hochfahren des Systems die Systemkonfiguration wieder her
 - a) Stellen Sie die Sicherung mithilfe der Wiederherstellungsfunktion wieder her
 9. Importieren Sie nach dem Hochfahren des Systems manuell die neue Lizenzdatei in das V3-System

25.4.3 Wie Sie PayGo-lizenzierte Systeme auf ein V3-Mainboard migrieren

Führen Sie folgende Migrationsschritte der Reihe nach durch:

Schritt für Schritt

1. Sichern Sie die Systemkonfiguration und die Kundendaten.
2. Generieren Sie die Lizenzdatei auf dem zentralen Lizenzserver (CLS) neu
 - a) Generieren Sie erneut eine neue Lizenzdatei für die MAC-Adresse auf dem V3-Mainboard
Übertragen Sie die bestehenden Lizenzen von der MAC-Adresse des V2-Mainboards auf die MAC-Adresse des V3-Mainboards.
 - b) Laden Sie die neue Lizenzdatei vom CLS herunter
3. Tauschen Sie die Mainboards

- a) Fahren Sie das System herunter und schalten Sie alle Versorgungsspannungen aus
 - b) Verwenden Sie V3-Datenträger und ggf. optionale Massenspeicher auf dem V3-Mainboard
 - c) Entfernen Sie die OCCB Voice Channel Booster Karte vom V2-Mainboard und stecken Sie sie in das V3-Mainboard ein.
 - d) Ersetzen Sie das V2-Mainboard im System durch das V3-Mainboard
 - e) Schalten Sie die Versorgungsspannungen wieder ein
Das System startet automatisch.
4. Stellen Sie nach dem Hochfahren die grundlegenden Systemparameter in WBM ein
 - a) Stellen Sie Systemdatum und -uhrzeit ein
 - b) Stellen Sie das Anwendungspaket ein
UC Smart für System ohne UC oder mit UC Smart
UC Suite für Systeme mit UC Suite
 5. Stellen Sie nach dem Hochfahren des Systems die Systemkonfiguration wieder her
 - a) Stellen Sie die Sicherung mithilfe der Wiederherstellungsfunktion wieder her
 6. Importieren Sie manuell die neue Lizenzdatei in das V3-System und aktivieren Sie die Lizenzdatei

25.5 Software-Aktualisierung von OpenScape Business S

Bestimmen Sie vor der Aktualisierung der OpenScape Business S System-Software die aktuelle Systemkonfiguration und ggf. die zu ersetzenden HW-/SW- und Lizenzkomponenten.

Tabelle 34: Migration von OpenScape Business S - HW-/SW-Checkliste

Komponenten	Ersetzt durch
Hardwarekomponenten	
Server-PC	Wiederverwendung ist möglich. Die HW-Anforderungen müssen für OpenScape Business S-Erweiterungen geprüft werden. ¹¹
Optipoint 400 Telefone	OpenScape Deskphone CP Telefone
Softwarekomponenten	

¹¹ Die bestehende PC-HW kann verwendet werden, wenn das UC Booster Server System nach der SW-Aktualisierung unverändert bleibt. Wenn nach der SW-Aktualisierung Erweiterungen geplant sind, müssen die Hardwareanforderungen ggf. gemäß den Spezifikationen in *OpenScape Business S Installationsanleitung, Kapitel Voraussetzungen* angepasst werden.

Komponenten	Ersetzt durch
Betriebssystem SLES12	Wiederverwendung ist möglich. Schließlich ist eine Aktualisierung auf das neueste Service Pack erforderlich ¹²
V2 System-SW auf SDHC-Karte	V3 System-SW (Image vom Software Download Server)
XMPP	Keine Follow-on-Lösung
myPortal Smart	myPortal @work
Lizenzkomponenten	
Lizenzen in Lizenzdatei	Übertragung der Lizenzen in eine neue Lizenzdatei
CSTA-Applikation (über UC Booster Card / Server)	CSTA-Applikation (über UC Booster Card / Server)

25.5.1 Software-Aktualisierung von OpenScape Business S V2 auf OpenScape Business S V3

Bei der Aktualisierung eines OpenScape Business S-Modells von SW-Version V2 auf V3 wird nur die System-SW ausgetauscht.

Bestehende Lizenzen und die Kundenkonfiguration werden übernommen. Der bestehende Software-Support wird nach der Migration unverändert fortgeführt.

In diesem Fall sind keine separaten Bestellpositionen für die System-SW-Aktualisierung von V2 auf V3 erforderlich.

Beachten Sie, dass die SW-Version V3 bestimmte Funktionen und Hardwarekomponenten nicht mehr unterstützt. In [Tabelle 34: Migration von OpenScape Business S - HW-/SW-Checkliste](#) auf Seite 779 finden Sie Informationen darüber, welche Komponenten in Version V3 ersetzt werden und welche Komponenten ohne Ersatz entfallen. Das hängt von der Ausbaustufe des Kundensystems ab.

¹² Das auf dem Server-PC installierte SLES-Betriebssystem kann im Fall einer SW-Aktualisierung von OpenScape Business S/UC Booster Server angepasst werden. Allerdings sollte vor der SW-Aktualisierung auf das letzte veröffentlichte Service Pack aktualisiert werden.

Wenn Novell den SW-Support für die verwendete SLES-Version eingestellt hat, muss der Kunde informiert und ggf. eine SLES-Aktualisierung verkauft werden.

Die SLES-Aktualisierung muss möglicherweise in mehreren Schritten durchgeführt werden, um bestehende Installationen von OpenScape Business S gemeinsam mit der Kundenkonfiguration und den Kundendaten zu übernehmen. Ein vorhandener SLES Update Key bleibt mit einer SLES-Aktualisierung gültig. Seine Registrierung bei Novell muss jedoch ggf. vor der SLES-Aktualisierung aufgehoben werden, bevor er für das neue System erneut registriert wird.

Im Folgenden wird die SW-Aktualisierung von OpenScape Business unter Beibehaltung des SLES-Betriebssystems beschrieben.

Voraussetzungen

Das System wird vor der Aktualisierung mit der zuletzt veröffentlichten SW-Version V2R7 betrieben. Aktualisieren Sie ggf. das System auf die neueste SW-Version. Dazu muss das System über einen gültigen Software-Support-Status verfügen.

Vor der Software-Aktualisierung von Version V2 auf V3 müssen Sie im System einen permanenten Zugang zum Unify-Lizenzserver einrichten (über das Internet) und die Funktion **CLS Connect** aktivieren.

Bedingungen und Einschränkungen für funktionale Grenzen

Bestehende Lizenzen können im Verlauf der SW-Aktualisierung nur übernommen werden, wenn die Funktion CLS Connect aktiviert ist.

Die Kundenkonfiguration und die Kundendaten werden beim SW-Aktualisierungsprozess von SW-Version V2 auf V3 automatisch übertragen.

Die wichtigsten technischen Schritte der Migration werden in den folgenden Kapiteln beschrieben. Um die bestehenden Lizenzen beizubehalten, wird folgende Unterscheidung in der Handhabung gemacht:

- SW-Aktualisierung für permanente Lizenzierung mit und ohne CLS Connect
- SW-Aktualisierung mit PayGo-Lizenzierung

Technische Abwicklung der Aktualisierung

Die wichtigsten technischen Schritte der Aktualisierung werden nachfolgend beschrieben. Es wird unterschieden zwischen

- Aktualisierung für permanente Lizenzierung mit CLS Connect
- Aktualisierung mit PayGo-Lizenzierung

25.5.1.1 Wie Sie permanent lizenzierte Systeme mit CLS Connect auf V3 aktualisieren

Führen Sie folgende Migrationsschritte durch:

Schritt für Schritt

1. Bereiten Sie das OpenScape Business V2 System vor
 - a) Aktualisieren Sie das vorhandene System auf SW-Version V2R7
 - b) Richten Sie im System einen Zugang zum zentralen Lizenzserver (Central License Server, CLS) ein und testen Sie die Verbindung
 - c) Aktivieren Sie CLS Connect im V2-System
2. Bereiten Sie das SLES-Betriebssystem vor
Aktualisieren Sie das Betriebssystem von der in Verbindung mit OpenScape Business S verwendeten SLES-Version auf das zuletzt veröffentlichte Service Pack.
3. Aktualisieren Sie die OpenScape Business-Software

- a) Führen Sie die Softwareaktualisierung auf V3 über OpenScape Business Assistant durch.
 - b) Die Systemkonfiguration wird automatisch auf V3 übertragen.
 - c) Bestehende Lizenzen werden auf V3 übertragen.
- 4.** Die Lizenzdatei wird automatisch vom zentralen Lizenzserver (CLS) generiert
- a) Nach dem Neustart des Systems überträgt das System die Information, dass die bestehenden Lizenzen mit Softwareversion 3 betrieben werden.
 - b) Der Lizenzserver generiert automatisch eine neue Lizenzdatei mit den V3-Informationen und überträgt sie zurück an das System.

25.5.1.2 Wie Sie PayGo-lizenzierte Systeme auf V3 aktualisieren

Führen Sie folgende Migrationsschritte durch:

Schritt für Schritt

- 1.** Bereiten Sie das OpenScape Business System vor
 - a) Aktualisieren Sie das vorhandene System auf SW-Version V2R7
- 2.** Bereiten Sie das SLES-Betriebssystem vor
Aktualisieren Sie das Betriebssystem von der in Verbindung mit OpenScape Business S verwendeten SLES-Version auf das zuletzt veröffentlichte Service Pack.
- 3.** Generieren Sie die Lizenzdatei auf dem zentralen Lizenzserver (CLS) neu
 - a) Generieren Sie erneut eine neue Lizenzdatei für das V2-System
 - b) Laden Sie die neue Lizenzdatei vom CLS herunter
- 4.** Importieren Sie die neue Lizenzdatei in das OpenScape Business V2-System und aktivieren Sie sie.
- 5.** Aktualisieren Sie die OpenScape Business-Software
 - a) Führen Sie die Softwareaktualisierung auf V3 über OpenScape Business Assistant durch.
 - b) Die Systemkonfiguration wird automatisch auf V3 übertragen.
 - c) Das System ist nach einem Neustart betriebsbereit.

25.5.2 Software-Aktualisierung von OpenScape Business S V2 auf OpenScape Business S V3

Um ein OpenScape Business S V1 System auf ein OpenScape Business S V2 System zu aktualisieren, sind die nachstehend beschriebenen Migrationsschritte durchzuführen.

Voraussetzungen

Vor der Migration ist zu prüfen, ob die Hard- und Softwareeigenschaften des Linux-Servers für OpenScape Business S V2 ausreichend sind. Ggf. reicht eine Aktualisierung des Linux Servers aus (z. B. mehr verfügbarer Arbeitsspeicher). Das für OpenScape

Business V2 veröffentlichte SLES 64-Bit-Linux-Betriebssystem ist eine Voraussetzung. Für den Aktualisierungsschritt auf OpenScape Business SW-Version V3 ist die für V3 veröffentlichte SLES 64-Bit-Version erforderlich.

Wird ein neuer Linux Server benötigt, ist nach der Linux-Installation die OpenScape Business V1 S Kommunikationssoftware zu installieren. Eine V1-Datensicherung kann übernommen werden und Sie können anschließend mit der Migration Schritt 1 fortfahren.

Bedingungen und Einschränkungen für funktionale Grenzen

Wenn das System von OpenScape Business V1 auf OpenScape Business V2 aktualisiert wird, ist eine ITSP-Aktivierung/Deaktivierung im Internet-Telefonie-Wizard erst dann möglich, wenn ein LCR-Reset durchgeführt wurde. Bereits in OpenScape Business V1 konfigurierte ITSPs funktionieren weiterhin in OpenScape Business V3 ohne LCR-Reset. Der bereits aktivierte ITSP kann bearbeitet jedoch nicht deaktiviert werden. Um im Wizard eine Änderung an der Aktivierung/Deaktivierung vorzunehmen, ist ein LCR-Reset erforderlich. Dies soll die nötigen Änderungen für die Erhöhung der ITSPs von 4 auf 8 widerspiegeln. Gehen Sie für das LCR-Reset zu **Experten-Modus > LCR > LCR-Flags** und klicken Sie auf das Flag **LCR-Daten zurücksetzen**.

Aktualisierungsvorgang

Führen Sie folgende Aktualisierungsschritte durch:

1) OpenScape Business V1 Software aktualisieren

Aktualisieren Sie mithilfe des WBM die OpenScape Business V1 Software auf die Version V1 R3.3 oder höher (siehe [Update des Kommunikationssystems](#) auf Seite 711).

2) OpenScape Business V2 Lizenzdatei laden

Laden Sie die OpenScape Business V2 Lizenzdatei in das OpenScape Business V1 System und aktivieren Sie die Lizenzen (siehe [Lizenzaktivierung \(Standalone\)](#) auf Seite 167).

Die Lizenz für die kostenfreien SLES Upgrades kann weiterhin genutzt werden.

3) Aktuelle OS Biz V2 Software laden

Laden Sie mit Hilfe des WBM die aktuelle OpenScape Business V2 Software in das Kommunikationssystem. Die V1-Daten werden dabei automatisch in V3-Daten konvertiert (siehe [Update des Kommunikationssystems](#) auf Seite 711).

4) Datensicherung durchführen

Sichern Sie Ihre V2-Daten (siehe [Sofortiges Sichern](#) auf Seite 707).

25.6 OpenScape Business V2 Netzwerk-Migration/-Aktualisierung auf V3

Bei der Migration oder Aktualisierung eines OpenScape Business Netzwerks auf V3 müssen alle Knoten im Netzwerk auf die SW-

Version V3 aktualisiert werden. Für die Netzwerkfunktionen ist es unerheblich, ob die SW-Version V3 auf einem OpenScape Business X System im Netzwerk mit einem V2-Mainboard oder einem V3-Mainboard betrieben wird.

Aktualisieren Sie jeden OpenScape Business Knoten im Netzwerk getrennt. Die für eine Aktualisierung erforderlichen Komponenten werden pro Knoten je nach den einzelnen Knoten gemäß den Beschreibungen in den Kapiteln [Software-Aktualisierung für OpenScape Business X Systeme](#) auf Seite 762, [Software-Aktualisierung von UC Booster Server auf OpenScape Business X V3](#) auf Seite 765, [Hardware/Software-Migration von OpenScape Business X Systemen auf V3](#) auf Seite 768 oder [OpenScape Business X V3 System von einem V2-Mainboard auf ein V3-Mainboard migrieren](#) auf Seite 774 bestimmt.

Die Lizenzen für die Knoten im V2-Netzwerk können über den zentralen Lizenzserver auf die V3-Systeme übertragen werden. Es gibt verschiedene Verfahren für Systeme mit der oder ohne die Funktion **CLS Connect**. Das Verfahren für die „Pay as you go“-Lizenzierung wird im OpenScape Business Netzwerk nicht unterstützt.

Der erforderliche Aufwand für die Übertragung von Lizenzen mit **CLS Connect** ist in einem Netzwerk erheblich geringer als ohne die Funktion CLS Connect.

Wichtig: Aktualisieren Sie die Knoten in einem Netzwerk in der für jedes Szenario beschriebenen Reihenfolge. Es ist wichtig, dass alle Slave-Knoten mit der Softwareversion V3 betrieben werden, bevor der Master-Knoten auf die Softwareversion V3 migriert oder aktualisiert werden kann.

Während der Netzwerkaktualisierung kommt es zu einem heterogenen Netzwerk, auf dem vorübergehend die Software V2 und V3 läuft. Während dieser Zeit kann die volle Funktionalität des Leistungsspektrums im Netzwerk nicht garantiert werden. In einigen Szenarien arbeiten die aktualisierten/migrierten Systeme nur im Notbetrieb bis die Lizenzdatei vom Master-Knoten aktualisiert wird.

OpenScape Business Netzwerke können in verschiedenen Kombinationen in Bezug auf die Verwendung von OpenScape Business X und S Systemen und die Lizenzierung der Systeme im Netzwerk realisiert werden. Die wichtigsten Schritte für die Migration oder Aktualisierung eines OpenScape Business Netzwerks und ihre Reihenfolge werden anhand von typischen Kombinationen gezeigt.

Die Beschreibung geht immer davon aus, dass eine Netzwerklizenzdatei für das Netzwerk auf dem zentralen Lizenzserver vorhanden ist, durch die der Master-Knoten alle Slave-Knoten mit Lizenzinformationen versorgt.

- **Netzwerk nur bestehend aus OpenScape Business X Systemen**

- Szenario 1: HW-Migration nur auf dem Master-Knoten, SW-Aktualisierung auf allen Slave-Knoten
- Szenario 2: SW-Aktualisierung für alle OpenScape Business X Knoten im Netzwerk
- **Netzwerk bestehend aus OpenScape Business S und OpenScape Business X Systemen**
 - Szenario 3: OpenScape Business S ist Master-Knoten und OpenScape Business X Systeme sind Slave-Knoten
 - Szenario 3a: SW-Aktualisierung für alle OpenScape Business Knoten im Netzwerk
 - Szenario 3b: SW-Aktualisierung auf dem OpenScape Business S Master-Knoten, Migration der Slave-Knoten

25.6.1 Szenario 1: Hardware-Migration von Master-Knoten, Software-Aktualisierung von Slave-Knoten

Bei der Migration des Netzwerks muss unterschieden werden zwischen der Funktion **CLS Connect** und dem Lizenzübertragungsverfahren.

25.6.1.1 Migration/Aktualisierung mit CLS Connect auf dem Master-Knoten

Voraussetzungen

- Alle Knoten im Netzwerk werden mit der zuletzt veröffentlichten SW-Version V2R7.x betrieben.
- Auf dem zentralen Lizenzserver (CLS) gibt es eine zentrale Netzwerklizenzdatei für den Master-Knoten des Netzwerks.
- Die Funktion **CLS Connect** ist auf dem Master-Knoten aktiviert. CLS Connect muss auf den Slave-Knoten nicht eingeschaltet werden.

Schritt für Schritt

1. Aktualisieren Sie alle Slave-Knoten auf die Softwareversion V3 (Details siehe [Software-Aktualisierung für OpenScape Business X Systeme](#) auf Seite 762 oder [Software-Aktualisierung von UC Booster Server auf OpenScape Business X V3](#) auf Seite 765)
 - a) Importieren Sie die V3-Software über den OpenScape Business Assistant (WBM) und aktualisieren Sie das System.
 - b) Die Konfiguration und die Lizenzinformationen bleiben erhalten. Das System ist nach dem Start aufgrund einer ungültigen Lizenzdatei nicht betriebsbereit.
2. Generieren Sie eine neue Netzwerklizenzdatei auf dem Lizenzserver.
 - a) Generieren Sie erneut die Netzwerklizenzdatei für die MAC-Adresse des V3-Mainboards
 - b) Laden Sie die neue Netzwerklizenzdatei vom CLS herunter

3. Migrieren Sie den Master-Knoten auf das V3-Mainboard (Details siehe [Hardware/Software-Migration von OpenScape Business X Systemen auf V3](#) auf Seite 768)
 - a) Sichern Sie die Systemkonfiguration über WBM
 - b) Tauschen Sie das Mainboard aus
 - c) Stellen Sie Datum/Uhrzeit und Anwendungspaket über WBM ein
 - d) Importieren und aktivieren Sie die neue Netzwerklizenzdatei über WBM.
 - e) Stellen Sie die Systemkonfiguration über WBM wieder her
Die Lizenzdatei wird in diesem Fall nicht überschrieben.
4. Der Master-Knoten überträgt die neuen Lizenzinformationen automatisch an die Slave-Knoten.

Anmerkung: Diese Übertragung der Lizenzen auf die Slave-Knoten kann bis zu 15 Minuten dauern.

25.6.1.2 Migration/Aktualisierung ohne CLS Connect auf dem Master-Knoten

Voraussetzungen

- Alle Knoten im Netzwerk werden mit der zuletzt veröffentlichten SW-Version V2R7.x betrieben.
- Auf dem zentralen Lizenzserver (CLS) gibt es eine zentrale Netzwerklizenzdatei für den Master-Knoten des Netzwerks.
- Hardware-Migrationslizenz-für Master-Knoten ist verfügbar
- Software-Upgrade-Lizenzen sind für jeden Slave-Knoten verfügbar

Schritt für Schritt

1. Generieren Sie die neue Netzwerklizenzdatei auf dem Lizenzserver
 - a) Unterteilen Sie die Netzwerkdatei auf dem CLS in einzelne Lizenzdateien
 - b) Generieren Sie eine Lizenzdatei für den Master-Knoten
Aktivieren Sie die Hardware-Migrationslizenz für den Master-Knoten
 - c) Generieren Sie die Lizenzdatei für die Slave-Knoten
Aktivieren Sie die Software-Upgrade-Lizenz für jeden einzelnen Slave-Knoten
 - d) Führen Sie die einzelnen Knotenlizenzdateien zu einer neuen Netzwerklizenzdatei zusammen
 - e) Laden Sie die neue Netzwerklizenzdatei vom CLS herunter
2. Aktualisieren Sie die Slave-Knoten auf V3 (Details siehe [Software-Aktualisierung für OpenScape Business X Systeme](#) auf Seite 762 oder [Software-Aktualisierung von UC Booster Server auf OpenScape Business X V3](#) auf Seite 765)
 - a) Importieren Sie die V3-Software über den OpenScape Business Assistant (WBM) und aktualisieren Sie das System.
 - b) Die Konfiguration und die Lizenzinformationen werden automatisch übertragen.

Das System ist nach dem Start aufgrund einer ungültigen Lizenzdatei nicht betriebsbereit.

3. Migrieren Sie den Master-Knoten nach V3 (Details siehe [Hardware/Software-Migration von OpenScape Business X Systemen auf V3](#) auf Seite 768)
 - a) Sichern Sie die Systemkonfiguration über WBM
 - b) Wechseln Sie das Mainboard
 - c) Stellen Sie Datum/Uhrzeit und Anwendungspaket über WBM ein
 - d) Importieren und aktivieren Sie die neue Netzwerklizenzdatei über WBM.
 - e) Stellen Sie die Systemkonfiguration über WBM wieder her (die Lizenzdatei wird in diesem Fall nicht überschrieben)
4. Der Master-Knoten überträgt die neuen Lizenzinformationen automatisch an die Slave-Knoten.

Anmerkung: Diese Übertragung der Lizenzen auf die Slave-Knoten kann bis zu 15 Minuten dauern.

25.6.2 Szenario 2: Software-Aktualisierung aller Systeme im Netzwerk auf V3

Bei der Aktualisierung der Netzwerksoftware definiert die Verwendung der Funktion **CLS Connect** oder nicht das zu befolgende Verfahren für die Übertragung der Lizenz.

25.6.2.1 Software-Aktualisierung mit CLS Connect auf dem Master-Knoten

Voraussetzungen

- Alle Knoten im Netzwerk werden mit der zuletzt veröffentlichten SW-Version V2R7.x betrieben.
- Auf dem zentralen Lizenzserver (CLS) gibt es eine zentrale Netzwerklizenzdatei für den Master-Knoten des Netzwerks.
- Die Funktion **CLS Connect** ist auf dem Master-Knoten aktiviert. CLS Connect muss auf den Slave-Knoten nicht eingeschaltet werden.

Schritt für Schritt

1. Migrieren Sie alle Slave-Knoten auf die Softwareversion V3 (Details siehe [Software-Aktualisierung für OpenScape Business X Systeme](#) auf Seite 762 oder [Software-Aktualisierung von UC Booster Server auf OpenScape Business X V3](#) auf Seite 765)
 - a) Importieren Sie die V3-Software über den OpenScape Business Assistant (WBM) und aktualisieren Sie das System.
 - b) Die Konfiguration und die Lizenzinformationen bleiben erhalten. Das System ist nach dem Start aufgrund einer ungültigen Lizenzdatei nicht betriebsbereit.

2. Aktualisieren Sie den Master-Knoten auf V3 (Details siehe [Software-Aktualisierung für OpenScape Business X Systeme](#) auf Seite 762 oder [Software-Aktualisierung von UC Booster Server auf OpenScape Business X V3](#) auf Seite 765)
 - a) Importieren Sie die V3-Software über den OpenScape Business Assistant (WBM) und aktualisieren Sie das System.
 - b) Die Konfiguration und die Lizenzinformationen bleiben erhalten.
 - c) Sie das System neu.
3. Die folgenden Schritte werden automatisch durchgeführt (kein manueller Eingriff erforderlich)
 - a) Der Master-Knoten meldet sich nach dem Start am CLS mit der Softwareversion 3.
 - b) Der CLS generiert eine neue Netzwerklizenzdatei.
 - c) Der CLS überträgt die neue Netzwerklizenzdatei an den Master-Knoten.
 - d) Der Master-Knoten überträgt die neuen Lizenzinformationen automatisch an die Slave-Knoten.

Anmerkung: Diese Übertragung der Lizenzen auf die Slave-Knoten kann bis zu 15 Minuten dauern.

25.6.2.2 Software-Aktualisierung ohne CLS Connect auf dem Master-Knoten

Voraussetzungen

- Alle Knoten im Netzwerk werden mit der zuletzt veröffentlichten SW-Version V2R7.x betrieben.
- Auf dem zentralen Lizenzserver (CLS) gibt es eine zentrale Netzwerklizenzdatei für den Master-Knoten des Netzwerks.
- Software-Upgrade-Lizenzen sind für jeden Knoten verfügbar

Schritt für Schritt

1. Generieren Sie neue Netzwerklizenzdateien auf dem Lizenzserver
 - a) Unterteilen Sie die Netzwerkdatei auf dem CLS in einzelne Lizenzdateien
 - b) Generieren Sie eine Lizenzdatei für den Master-Knoten
Aktivieren Sie die Software-Upgrade-Lizenz für den Master-Knoten
 - c) Generieren Sie die Lizenzdatei für die Slave-Knoten
Aktivieren Sie die Software-Upgrade-Lizenz für jeden einzelnen Slave-Knoten
 - d) Führen Sie die einzelnen Knotenlizenzdateien zu einer neuen Netzwerklizenzdatei zusammen
 - e) Laden Sie die neue Netzwerklizenzdatei vom CLS herunter
2. Migrieren Sie alle Slave-Knoten auf V3 (Details siehe [Software-Aktualisierung für OpenScape Business X Systeme](#) auf Seite 762 oder [Software-Aktualisierung von UC Booster Server auf OpenScape Business X V3](#) auf Seite 765)

- a) Importieren Sie die V3-Software über den OpenScape Business Assistant (WBM) und aktualisieren Sie das System.
- b) Die Konfiguration und die Lizenzinformationen bleiben erhalten.
- c) Das System ist nach dem Start aufgrund einer ungültigen Lizenzdatei nicht betriebsbereit.

Das System ist nach dem Start aufgrund einer ungültigen Lizenzdatei nicht betriebsbereit.

3. Aktualisieren Sie den Master-Knoten auf V3 (Details siehe [Software-Aktualisierung für OpenScape Business X Systeme](#) auf Seite 762 oder [Software-Aktualisierung von UC Booster Server auf OpenScape Business X V3](#) auf Seite 765)
 - a) Importieren Sie die V3-Software über den OpenScape Business Assistant (WBM) und aktualisieren Sie das System.
 - b) Die Konfiguration und die Lizenzinformationen bleiben erhalten.
 - c) Importieren Sie die Netzwerklizenzdatei in den Master-Knoten und aktivieren Sie die Lizenzdatei
4. Der Master-Knoten überträgt die neuen Lizenzinformationen automatisch an die Slave-Knoten.

Anmerkung: Diese Übertragung der Lizenzen auf die Slave-Knoten kann bis zu 15 Minuten dauern.

25.6.3 Szenario 3a: Software-Aktualisierung aller Knoten

In diesem Szenario ist der Master-Knoten ein OpenScape Business S System und die Slave-Knoten sind OpenScape Business X Systeme.

Dieses Szenario ist identisch mit [Szenario 2: Software-Aktualisierung aller Systeme im Netzwerk auf V3](#) auf Seite 787

25.6.4 Szenario 3b: Software-Aktualisierung auf dem Master-Knoten, Hardware-Migration auf den Slave-Knoten

In diesem Szenario werden die Slave-Knoten durch einen HW-/SW-Austausch auf das V3-Mainboard und die SW-Version 3 migriert. Im OpenScape Business S Master-System wird die SW von V2 auf V3 aktualisiert. Für die HW-/SW-Aktualisierung des Netzwerks definiert die Verwendung der Funktion CLS Connect das Lizenzübertragungsverfahren.

25.6.4.1 Migration/Aktualisierung mit CLS Connect auf dem Master-Knoten

Voraussetzungen

- Alle Knoten im Netzwerk werden mit der zuletzt veröffentlichten SW-Version V2R7.x betrieben.
- Auf dem zentralen Lizenzserver (CLS) gibt es eine zentrale Netzwerklizenzdatei für den Master-Knoten des Netzwerks.

- Die Funktion **CLS Connect** ist auf dem Master-Knoten aktiviert. CLS Connect muss auf den Slave-Knoten nicht eingeschaltet werden.
- Die V3-Mainboards einschließlich der V3-Software sind verfügbar.

Schritt für Schritt

1. Migrieren Sie alle Slave-Knoten auf das V3-Mainboard (Details siehe [Hardware/Software-Migration von OpenScape Business X Systemen auf V3](#) auf Seite 768)
 - a) Sichern Sie die Systemkonfiguration über WBM
 - b) Ersetzen Sie die Mainboards
 - c) Stellen Sie Datum/Uhrzeit und Anwendungspaket über WBM ein
 - d) Stellen Sie die Systemkonfiguration über WBM wieder her
Das System ist nach dem Start aufgrund einer ungültigen Lizenzdatei nicht betriebsbereit.
2. Aktualisieren Sie den Master-Knoten auf V3 (Details siehe [Software-Aktualisierung für OpenScape Business X Systeme](#) auf Seite 762 oder [Software-Aktualisierung von UC Booster Server auf OpenScape Business X V3](#) auf Seite 765)
 - a) Importieren Sie die V3-Software über den OpenScape Business Assistant (WBM) und aktualisieren Sie das System.
 - b) Die Konfiguration und die Lizenzinformationen bleiben erhalten.
 - c) Sie das System neu.
3. Die folgenden Schritte werden automatisch durchgeführt (kein manueller Eingriff erforderlich)
 - a) Der Master-Knoten meldet sich nach dem Start am CLS mit der Softwareversion 3.
 - b) Der CLS generiert eine neue Netzwerklizenzdatei.
 - c) Der CLS überträgt die neue Netzwerklizenzdatei an den Master-Knoten.
 - d) Der Master-Knoten überträgt die neuen Lizenzinformationen automatisch an die Slave-Knoten.

Anmerkung: Diese Übertragung der Lizenzen auf die Slave-Knoten kann bis zu 15 Minuten dauern.

25.6.4.2 Migration/Aktualisierung ohne CLS Connect auf dem Master-Knoten

Voraussetzungen

- Alle Knoten im Netzwerk werden mit der zuletzt veröffentlichten SW-Version V2R7.x betrieben.
- Auf dem zentralen Lizenzserver (CLS) gibt es eine zentrale Netzwerklizenzdatei für den Master-Knoten des Netzwerks.
- Die Software-Upgrade-Lizenz für den Master-Knoten ist verfügbar
- Hardware-Migrationslizenzen sind für jeden Slave-Knoten verfügbar
- Die V3-Mainboards einschließlich der V3-Software sind verfügbar.

Schritt für Schritt

1. Generieren Sie eine neue Netzwerklizenzdatei auf dem Lizenzserver
 - a) Unterteilen Sie die Netzwerkdatei auf dem CLS in einzelne Lizenzdateien
 - b) Generieren Sie eine Lizenzdatei für den Master-Knoten
Aktivieren Sie die Software-Upgrade-Lizenz für den Master-Knoten
 - c) Generieren Sie die Lizenzdatei für die Slave-Knoten
Aktivieren Sie die Hardware-Migrationslizenz für jeden Slave-Knoten
 - d) Führen Sie die einzelnen Knotenlizenzdateien zu einer neuen Netzwerklizenzdatei zusammen
 - e) Laden Sie die neue Netzwerklizenzdatei vom CLS herunter
2. Migrieren Sie alle Slave-Knoten auf das V3-Mainboard (Details siehe [Hardware/Software-Migration von OpenScape Business X Systemen auf V3](#) auf Seite 768)
 - a) Sichern Sie die Systemkonfiguration über WBM
 - b) Ersetzen Sie die Mainboards
 - c) Stellen Sie Datum/Uhrzeit und Anwendungspaket über WBM ein
 - d) Stellen Sie die Systemkonfiguration über WBM wieder her
Das System ist nach dem Start aufgrund einer ungültigen Lizenzdatei nicht betriebsbereit.
3. Aktualisieren Sie den Master-Knoten auf V3 (Details siehe [Software-Aktualisierung für OpenScape Business X Systeme](#) auf Seite 762 oder [Software-Aktualisierung von UC Booster Server auf OpenScape Business X V3](#) auf Seite 765)
 - a) Importieren Sie die V3-Software über den OpenScape Business Assistant (WBM) und aktualisieren Sie das System.
 - b) Die Konfiguration und die Lizenzinformationen bleiben erhalten.
 - c) Importieren Sie die Netzwerklizenzdatei in den Master-Knoten und aktivieren Sie die Lizenzdatei
4. Der Master-Knoten überträgt die neuen Lizenzinformationen automatisch an die Slave-Knoten.

Anmerkung: Diese Übertragung der Lizenzen auf die Slave-Knoten kann bis zu 15 Minuten dauern.

25.7 Migration von HiPath 3000 auf OpenScape Business V3

Beschrieben wird die technische Migration von HiPath 3000 / 500 V9 Standalone-Systemen und HiPath 3000 Netzverbunden auf OpenScape Business V3 mit V3-Mainboards.

Bei der Migration von HiPath 3000 Systemen nach OpenScape Business X V3 mit V3-Mainboards kann je nach Hardwarekonfiguration ein Teil der Hardwareausstattung des Systems und der angeschlossenen Terminals/Clients übertragen werden.

Vor der Migration von HiPath 3000 müssen die aktuelle Systemkonfiguration sowie ggf. die zu ersetzenden HW-/SW- und Lizenzkomponenten durch wiederholte Prüfungen bestimmt werden.

Allgemeine Prüfungen

- **Funktions-Kompatibilitätscheck**

Bitte informieren Sie sich, welche Funktionen gegenüber HiPath 3000 V9 nicht mehr unterstützt werden oder sich geändert haben. Kapitel [Geänderte/gestrichene Leistungsmerkmale und Schnittstellen von HiPath 3000](#) auf Seite 817 listet die Funktionen von HiPath 3000 auf, die in OpenScape Business nicht mehr unterstützt werden oder durch neuere Funktionen ersetzt wurden.

- **Prüfung der Softwareversion**

Das System muss vor der Migration unter SW-Version V9 betrieben werden. Systeme mit einer SW-Version vor V9 müssen vor der Migration auf SW-Version V9 aktualisiert und in Betrieb genommen werden.

- **Prüfung der Schutzerdung**

Für alle OpenScape Business X Kommunikationssysteme ist eine Schutzerdung über einen zusätzlichen Schutzleiter zwingend erforderlich!

Hardware-Kompatibilitätscheck

Einige Module und Endgeräte können aus technischen Gründen nicht in den OpenScape Business X Systemen eingesetzt werden. Bei der Migration von HiPath 3000 V9 auf OpenScape Business V3 müssen diese Module und Terminals entfernt werden. Verwenden Sie bei Bedarf stattdessen die jeweiligen Nachfolgetypen. Die Liste der nicht mehr unterstützten Module und deren Nachfolger finden Sie in der *OpenScape Business X3/X5/X8 Servicedokumentation* im Abschnitt *Nicht unterstützte HW-Komponenten*.

- **Netzteil**

OpenScape Business 33xx / 35xx kann mit UPSC-D/DR- oder OCPSM-Netzteil betrieben werden. Verbleibende PSU-Netzteile müssen mit OCPSM ersetzt werden. Geeignete PSU-Upgrade-Kits sind erhältlich.

- **Peripheriekomponenten**

Bitte überprüfen Sie, ob die vorhandene Hardware weiterhin verwendet werden kann. Nicht mehr unterstützte Module und Endgeräte müssen entfernt oder ggf. durch Nachfolger ersetzt werden.

- **Backplane-Prüfung**

In HiPath 3550 Systemen wird Steckplatz 10 der Backplane nicht mehr vom V3-Mainboard angesprochen. Vorhandene Peripheriemodule, die diesen Steckplatz nutzen, können in OpenScape Business nicht betrieben werden.

- **Prüfung der Telefongeräte**

OpenScape Business V3 Systeme mit V3-Mainboards unterstützen analoge, ISDN-, SIP- und OpenStage oder OpenScape Deskphone

IP-/CP-Geräte. Vorhandene Optiset E-, Optipoint 4xx- und Optipoint 5xx-Geräte müssen ersetzt werden.

- **Gehäuseprüfung**

Bei migrierten HiPath 33xx/35xx Systemen müssen gegebenenfalls die Gehäusedeckel ausgetauscht und Lüftereinheiten installiert werden.

Entsprechende Lieferpositionen sind erhältlich.

Sonstige Prüfungen

- **Rufnummernplan für vernetzte Systeme**

Bei reiner Sprachvernetzung ist die offene und die geschlossene Nummerierung möglich. Bei Nutzung von UC Suite ist eine geschlossene Nummerierung im Netzwerk erforderlich (netzweite UC-Funktionalität).

25.7.1 Migration von HiPath 33xx, 35xx, 3800 nach OpenScape Business X3/X5/X8 V3

Bei der Migration eines HiPath 33xx, 35xx oder 3800 Systems nach OpenScape Business X V3 werden das Mainboard, die ermittelten Peripheriegruppen und Endgeräte sowie die System-SW ersetzt. Vorhandene Lizenzen können mit einer Upgrade-Lizenz migriert werden. Die Systemkonfiguration kann übertragen werden. Nach der Migration hat das OpenScape Business V3 System 3 Jahre lang Software-Support.

Für die Migration von HiPath 3000 V9 nach OpenScape Business V3 sind grundsätzlich folgende Punkte erforderlich:

- V3-Mainboard
- V3 SW auf SSD-Datenspeicher
- M2 SSD 256 GB Massenspeicher (optional mit Applikation UC Suite)
- OpenScape Business Upgrade HiPath 3000 V9 (Lizenzmigration) oder
- OpenScape Business Upgrade HiPath 3000 V8 (Lizenzmigration) oder
- OpenScape Business Upgrade HiPath 3000 V7 (Lizenzmigration)
- OpenScape Business CSTA-Lizenz (optional)

Bei Bedarf müssen zusätzliche Hardwarekomponenten und Lizenzen bestellt werden. Das hängt von der Konfiguration des Kundensystems ab.

In der *OpenScape Business X3/X5/X8 Servicedokumentation* im Abschnitt *Nicht unterstützte HW-Komponenten* finden Sie Informationen darüber, welche Komponenten in der Version V3 ersetzt werden oder ersatzlos entfallen. Bitte beachten Sie, dass eine CSTA-Lizenz für eine bestehende Verbindung zu externen CSTA-Applikationen erforderlich ist. Das gilt nicht für die Verbindung zu OpenScape Business TAPI 170 oder TAPI 120.

Voraussetzungen

Alle HW-/SW-Komponenten wurden auf Wiederverwendbarkeit geprüft.

Alle neuen HW-/SW-Komponenten sind verfügbar

Eine Upgrade-Lizenz für die Aktualisierung von HiPath 3000 V7, V8 oder V9 auf OpenScape Business V3 wurde bestellt und der LAC der Upgrade-Lizenz ist vorhanden, um die neue Lizenz vom Lizenzserver abzurufen.

Das System wurde für die technische SW-Migration der Kundenkonfiguration auf die neueste SW-Version V9 aktualisiert.

Die neueste Version des Manager E wird verwendet

OpenScape Business Lizenzen während der Migration bestimmen

Die vorhandenen Lizenzen in HiPath 3000 können durch Aktivierung der Lizenz „OpenScape Business Upgrade HiPath 3000 (V7, V8 oder V9)“ auf dem zentralen Lizenzserver auf das OpenScape Business V3 System übertragen werden. Während der Lizenzübertragung wird eine neue Lizenzdatei für das OpenScape Business V3 System mit den folgenden Lizenzen erstellt:

Tabelle 35: HiPath 3000 Lizenzmigration

HP 3000 Lizenz	OpenScape Business Lizenz	Hinweise
	Basislizenz	Neu erstellt inkl. 3 Jahre SW-Support
	OpenDirectory Basislizenz	Neu erstellt
	Web Collaboration Connector Lizenz	Neu erstellt
	TDM Benutzerlizenz	Anzahl berechnet aus der Systemkonfiguration ¹³
IP-Teilnehmer (ComScendo)	IP Benutzerlizenz	1:1-Übertragung von HP 3000 Lizenzdatei
	TDM Benutzerlizenzierung	berechnet aus der Systemkonfiguration ¹³
S2M-Kanäle	IP/S2M/TI Trunk-Leitungslizenzen	1:1-Übertragung von HP 3000 Lizenzdatei
Mobility Entry	Mobility Benutzerlizenzen	1:1-Übertragung von HP 3000 Lizenzdatei
Xpressions Compact	Xpressions Compact Lizenzen ¹⁴	1:1-Übertragung von HP 3000 Lizenzdatei ¹⁴

¹³ Wird im Lauf der technischen Konvertierungsbeschreibung bestimmt, siehe unten.

Bestimmung der TDM Benutzerlizenzen innerhalb der Lizenzdatei

Während der technischen Konvertierung der HiPath 3000 Systemkonfiguration wird die Anzahl der aktiven TDM-Teilnehmer vom Tool Manager E bestimmt und in eine „Inventardatei (XML)“ geschrieben.

Die Anzahl der TDM User Lizenzen wird nach folgenden Regeln ermittelt:

- 1x TDM User Lizenz pro aktivem UP0-Port - Telefon (Master/Slave) bereit, Rufnummer verfügbar
- 1x TDM User Lizenz pro registriertem DECT-Telefon - Rufnummer verfügbar
- 1x TDM User Lizenz pro aktivem a/b-Port (Rufnummer) für gesteckte Baugruppen
- 1x TDM User Lizenz pro aktivem S0-Port (Rufnummer) für aktive Baugruppen

Die Migration der TDM Benutzerlizenz selbst wird offline am CLS über die XML-Inventardatei ausgeführt.

Der zentrale Lizenzserver prüft, ob eine Lizenzdatei für die MAC-Adresse des HiPath 3000 Mainboards vorhanden ist.

Wenn eine Lizenzdatei vorhanden ist, wird die Lizenzmigration auf Basis dieser Lizenzdatei und der Informationen in der „Inventardatei“ durchgeführt.

Wenn keine Lizenzdatei vorhanden ist, wird die Aktualisierung von OpenScape Business auf Basis der XML-„Inventardatei“ durchgeführt.

Je nach vorhandener Upgrade-Lizenz (V7, V8 oder V9) wird der folgende Prozentsatz der ermittelten TDM-Benutzer in OpenScape Business übernommen.

- Aktualisierung von HiPath 3000 V4 oder älter auf OpenScape Business V3:
TDM-Nutzer werden nicht für günstigere / kostenlose OpenScape Business-Upgrade-Lizenzen berechnet
- Aktualisierung von HiPath 3000 V5, V6 oder V7 auf OpenScape Business V3:
70% der TDM-Nutzer werden für günstigere / kostenlose OpenScape Business-Upgrade-Lizenzen berechnet.
- Aktualisierung von HiPath 3000 V8 auf OpenScape Business V3:
80% der TDM-Nutzer werden für günstigere / kostenlose OpenScape Business-Upgrade-Lizenzen berechnet.
- Aktualisierung von HiPath 3000 V9 auf OpenScape Business V3:
100% der TDM-Nutzer werden für günstigere / kostenlose OpenScape Business-Upgrade-Lizenzen berechnet.

¹⁴ Die Xpressions Compact Lizenzen sind in der Lizenzdatei enthalten, können aber in der SW-Version V3 nicht verwendet werden.

Bedingungen und Einschränkungen für funktionale Grenzen

- Die Lizenzmigration kann nur auf V3 erfolgen. Eine Lizenzmigration auf V2 wird vom Manager E nicht unterstützt.
- Die Lizenzmigration eines HiPath 3000 Systems (Mainboard) kann nur einmal durchgeführt werden und das Mainboard ist für weitere Aktionen nach der Migration am CLS gesperrt.
- Um S2M-Leitungen und ComScendo-Teilnehmer zu migrieren, muss eine HiPath 3000 Lizenzdatei auf dem zentralen Lizenzserver verfügbar sein.
- Die während der Migration generierten TDM-Benutzerlizenzen können nicht auf andere Systeme oder auf ein CLS-Konto übertragen werden.
- Benutzerlizenzen und UC benutzerbezogene Lizenzen werden Benutzern in OpenScape Business permanent zugewiesen. Bitte beachten Sie, dass für Benutzer von myAgent und myAttendant eine ausreichende Anzahl an Lizenzen zur Verfügung steht. In OpenScape Business sind Änderungen im Präsenzstatus anderer Benutzer durch Benutzer von myAgent an die myAttendant Lizenz gebunden. Diese sind separat zu bestellen.
- Das Leistungsmerkmal Deskshare User (IP-Mobility) ist in OpenScape Business lizenzpflichtig im Gegensatz zur HiPath 3000. Zusätzliche IP-Benutzerlizenzen müssen im OpenScape Business Assistant Lizenzierungsdialogfeld für die „Deskshare User“ vorhanden und diesen zugewiesen sein.
- Für folgende Produkte und Funktionen wird keine Lizenzmigration durchgeführt:
 - 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.
Nachfolgeprodukt: Smart Voicemail
 - myPortal entry Web Services Communications Clients auf dem Plug PC.
 - Basisstationen: 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 S0-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.

Technische Abwicklung

Führen Sie folgende Migrationschritte der Reihe nach durch:

1) HiPath 3000 Kundendatenbank (KDS) aus dem System herunterladen

Laden Sie mit Hilfe der neuesten Version von Manager E den aktuellen HiPath 3000 KDS aus dem HiPath 3000 System herunter.

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 KDS konvertieren

Konvertieren Sie mit Hilfe der neuesten Version von Manager E den aktuellen HiPath 3000 KDS in den OpenScape Business V3 KDS.

4) Hardware austauschen

Tauschen Sie das HiPath 3000 Mainboard gegen das neue OpenScape Business V3-Mainboard aus. Entfernen Sie auch alle HG1500 Baugruppen und alle nicht mehr unterstützten Unterbaugruppen. 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 Version von Manager E in das OpenScape Business V2 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 (z. B. Wahlpläne, Wegetabellen, Wahlregeln) auf die

Standardeinträge von OpenScape Business zurücksetzen. Diese Einstellung finden Sie im WBM im Wizard **Basisinstallation**.

25.7.1.1 Wie Sie den KDS aus HiPath 3000 laden

Voraussetzungen

Ein HiPath 3000 Kommunikationssystem (HiPath 3300, HiPath 3350, HiPath 3500, HiPath 3550 oder HiPath 3800) ist 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 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 Ordner Ihrer Wahl.

Nächste Schritte

[Wie Sie die HG1500 Einstellungen auslesen](#) auf Seite 798

25.7.1.2 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 KDS konvertieren](#) auf Seite 799

25.7.1.3 Wie Sie den HiPath 3000 KDS konvertieren

Voraussetzungen

Ein HiPath 3000 Kommunikationssystem (HiPath 3300, HiPath 3350, HiPath 3500, HiPath 3550 oder HiPath 3800) ist 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 **Name** und Ihre **Vertragsnummer** ein und klicken Sie auf **Weiter**.
4. Wählen Sie als **Version OpenScape Business V2** aus und klicken Sie auf **Weiter**.
5. Bestätigen Sie die Hinweise auf nicht mehr unterstützte Baugruppen mit **OK**.
6. Klicken Sie auf **Ja**, um das Infofenster mit der Anzahl der zu migrierenden TDM-Benutzer zu bestätigen und fahren Sie mit der Migration fort.
Die Anzahl der zu migrierenden TDM-Benutzer wird automatisch berechnet.
7. Bestätigen Sie die Anzeige der gesteckten Baugruppen mit **Weiter**.
8. Klicken Sie in der Menüleiste auf **Datei** > **KDS speichern** und speichern Sie den KDS unter einem anderen Namen auf dem Admin-PC in einem Ordner Ihrer Wahl.
9. Schließen Sie den Manager E.

Nächste Schritte

[Wie Sie die Hardware bei HiPath 3300/3500 austauschen](#) auf Seite 799 oder

[Wie Sie die Hardware bei HiPath 3350/3550 austauschen](#) auf Seite 801 oder

[Wie Sie die Hardware bei HiPath 3800 austauschen](#) auf Seite 802

25.7.1.4 Wie Sie die Hardware bei HiPath 3300/3500 austauschen

Voraussetzungen

Laufendes HiPath 3000 Kommunikationssystem für den Rackbetrieb (HiPath 3300 oder HiPath 3500).

OpenScape Business V3-Mainboard (OCCMRA oder OCCMRB).



Achtung:

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 V3-Mainboard.
9. Stecken Sie die M.2 SATA SSD mit System-SW und optional eine M.2 NVMe SDD auf das V3-Mainboard.
10. Stecken Sie optionale Module wie OCCBH oder OCCBL ein
11. Schieben Sie vorsichtig mit beiden Händen das OCCMRA- oder OCCMRB-Mainboard waagrecht in den Steckplatz des Baugruppenrahmens, wo vorher das HiPath 3000 Mainboard steckte.
12. Schließen Sie optionale Module wie STRBR an das V3-Mainboard an.
13. Stecken Sie wieder alle Stecker in das Mainboard, wie z.B. analoge Teilnehmer, ISDN-Leitungen, usw.

Anmerkung: 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.

14. Verbinden Sie Ihr Kommunikationssystem ordnungsgemäß mit dem Schutzleiter.
15. Stecken Sie den Netzstecker wieder ein und fahren Sie das System hoch.

Nächste Schritte

[Wie Sie die Erstinstallation durchführen](#) auf Seite 803

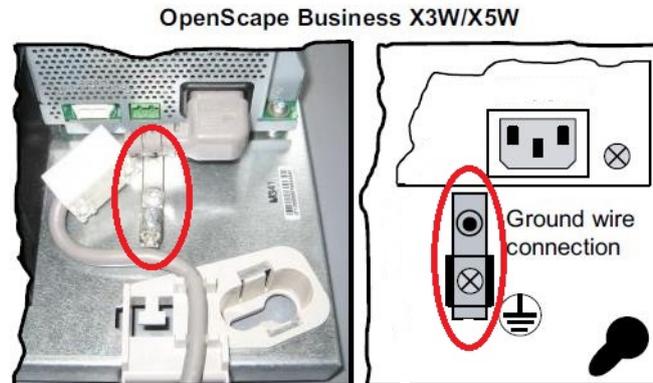
25.7.1.5 Wie Sie die Hardware bei HiPath 3350/3550 austauschen

Voraussetzungen

Laufendes HiPath 3000 Kommunikationssystem für den Wandbetrieb (HiPath 3350 oder HiPath 3550).

OpenScape Business Mainboard (OCCMA oder OCCMB).

Bei Migration von HiPath 3350/3550 zu OpenScape Business X3W/X5W muss die Schutzerdungsklemme installiert werden wie in der Abbildung unten gezeigt. Danach muss das Schutzerdungskabel wie in der Installationsanleitung beschreiben innerhalb von OpenScape Business V2 bzw. OpenScape Business X3/X5/X8 angeschlossen werden.



Achtung:

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. 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. Stecken Sie die M.2 SATA SSD mit System-SW und optional eine M.2 NVMe SSD auf das V3-Mainboard.
11. Stecken Sie optionale Module wie OCCBH oder OCCBL ein.
12. Stecken Sie vorsichtig das OpenScape Business OCCMA- oder OCCMB-Mainboard in den gleichen Slot, wo vorher das HiPath 3000 Mainboard steckte.
13. Schließen Sie optionale Module wie STRBR an das V3-Mainboard an.
14. 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.
15. Bringen Sie den neuen Baugruppenriegel an.
16. Verbinden Sie Ihr Kommunikationssystem ordnungsgemäß mit dem Schutzleiter.
17. Setzen Sie das Gehäuse auf und verriegeln Sie es.
18. Stecken Sie den Netzstecker wieder ein und fahren Sie das System hoch.

Nächste Schritte

[Wie Sie die Erstinstallation durchführen](#) auf Seite 803

25.7.1.6 Wie Sie die Hardware bei HiPath 3800 austauschen

Voraussetzungen

Laufendes HiPath 3800 Kommunikationssystem.

OpenScape Business Mainboard OCCLA.

**Achtung:**

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. Stecken Sie die M.2 SATA SSD mit System-SW und optional eine M.2 NVMe SDD auf das V3-Mainboard.
8. Stecken Sie optionale Module wie OCCBH oder OCCBL ein.
9. Stecken Sie vorsichtig das OpenScape Business OCCLA-Mainboard in den gleichen Slot, wo vorher das HiPath 3000 Mainboard steckte.
10. Stecken Sie wieder alle Stecker in das Mainboard.
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](#) auf Seite 803

25.7.1.7 Wie Sie die Erstinstallation durchführen

Die Erstinstallation des Kommunikationssystems wird in [Integration ins Kunden-LAN](#) beschrieben.

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](#) auf Seite 804

25.7.1.8 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 die Meldung mit **OK**.
5. Klicken Sie in der Menüleiste auf **Datei > Übertragen**.
6. Klicken Sie auf die Registerkarte **Kommunikation**.
7. Aktivieren Sie die Option **IP - HiPath** im Bereich **Zugang** 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](#) auf Seite 805

25.7.1.9 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 V2 Update HiPath 3000** und klicken Sie erneut auf **Generate Key**.

License Key Generation Details

Cancel Next >

Technical Details

With 'Verify' you can check your input data and view licenses that are already generated for this Locking ID (e.g.: MAC Address) in the detail section below.

CAUTION: For virtual systems the Advanced Locking ID has to be used. For hardware based systems the MAC address is of relevance.

To calculate the Advanced Locking ID click here: Calculate Locking ID

*Locking ID: Alias Name:

Locking ID of Network CLA:

Configuration File Content:

SIEL-ID: SID:1324300658865

Verify Prefill Details

OpenScape Business V1

Quantity to Use	Available Quantity	Existing Quantity New System	Max Quantity	Feature	Duration	Version	Type	Action
<input type="text" value="1"/>	1		1	OpenScape Business V1 Upgrade HiPath 3000 V9		V1	New License	To be activated

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.

Anmerkung: 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](#) auf Seite 807

25.7.1.10 Wie Sie die Lizenzdatei offline aktivieren

Die Offline-Lizenzaktivierung wird im Kapitel [Wie Sie Lizenzen offline aktivieren \(Standalone\)](#) beschrieben.

Nächste Schritte

[Wie Sie Lizenzen zuordnen](#) auf Seite 807

25.7.1.11 Wie Sie Lizenzen zuordnen

Die Lizenzzuordnung wird in [Lizenzzuordnung \(Standalone\)](#) auf Seite 168 beschrieben.

25.7.1.12 Wie Sie die LCR-Einträge zurücksetzen

Die Grundinstallation des Kommunikationssystems wird in [Basiskonfiguration](#) auf Seite 100 beschrieben).

Die Basisinstallation umfasst die Konfiguration der Systemrufnummer, der Teilnehmer sowie den Zugang zum Internet und die Internet-Telefonie.

Im Wizard **Grundinstallation** finden Sie im Fenster **Zentrale Teilnehmerfunktionen** ein zusätzliches Optionsfeld **Konfigurierte LCR-Daten löschen und mit LCR-Standarddaten initialisieren**. 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.

25.7.2 Migration eines HiPath 3000 Systems mit OpenScape Office V3 HX auf OpenScape Business V3 mit V3-Mainboard

Bei der Migration von HiPath 3000 Systemen mit einem angeschlossenen OpenScape Office HX Server ist der externe Server nicht erforderlich. Seine Funktion wird vom entsprechenden V3-Mainboard des OpenScape Business X Systems übernommen.

Das HiPath 3000 System wird migriert wie in [Migration von HiPath 33xx, 35xx, 3800 nach OpenScape Business X3/X5/X8 V3](#) auf Seite 793 beschrieben.

OpenScape Office HX Lizenzen sind Teil der HiPath 3000 Lizenzdatei. Daher werden sie im Verlauf der HiPath 3000 Lizenzmigration auch auf die OpenScape Business Lizenzen übertragen.

Anforderungen

Um OpenScape Business HX Lizenzen zu migrieren, muss eine HiPath 3000 Lizenzdatei auf dem zentralen Lizenzserver verfügbar sein.

Für die HiPath 3000 Lizenzen wird die Lizenzmigration durchgeführt wie in [Tabelle 35: HiPath 3000 Lizenzmigration](#) auf Seite 794 gezeigt. Das Folgende gilt für die OpenScape Office HX Lizenzmigration:

Tabelle 36: OpenScape Office HX Lizenzmigration

OpenScape Office HX Lizenz	OpenScape Business Lizenz	Hinweise
Pro Basislizenz	1x AutoAttendant Lizenz	
Pro OpenScape Office Standardbenutzer:	1x UC Benutzer 1x Voicemail Benutzer 1x Fax Benutzer	Gilt für alle Standardbenutzerlizenzen in den HX Basislizenzen 5/10 sowie für Single-User-Lizenzen
OpenScape Office HX Voicemail Lizenz	500 x Voicemail Benutzer	
myPortal for Outlook	Groupware User	Anzahl laut Lizenzdatei
myAttendant	myAttendant	Anzahl laut Lizenzdatei
myAgent	myAgent Benutzer	Anzahl laut Lizenzdatei
Contact Center Fax	Contact Center Fax Benutzer	Anzahl laut Lizenzdatei
Contact Center E-Mail	Contact Center E-Mail Benutzer	Anzahl laut Lizenzdatei
myReports	myReports	Anzahl laut Lizenzdatei
Application Launcher	Application Launcher	Anzahl laut Lizenzdatei
OpenDirectory Connector	OpenDirectory Connector	Anzahl laut Lizenzdatei

Bedingungen und Einschränkungen für funktionale Grenzen

Die Lizenzmigration kann nur auf V3 erfolgen. Eine Lizenzmigration auf V2 wird vom Manager E nicht unterstützt.

Die der Lizenzmigration ist nur einmal möglich.

Benutzerlizenzen und UC benutzerbezogene Lizenzen werden Benutzern in OpenScape Business permanent zugewiesen. Bitte beachten Sie, dass für Benutzer von myAgent und myAttendant eine ausreichende Anzahl an Lizenzen zur Verfügung steht.

In OpenScape Business sind Änderungen im Präsenzstatus anderer Benutzer durch Benutzer von myAgent an die myAttendant Lizenz gebunden. Diese sind separat zu bestellen.

Es ist nicht möglich, Ansagen, Bilder, Voicemails, Fax, Journal, Contact Center-Daten, Teilnehmerkonfiguration, Profile, externes Verzeichnis, Termine von OpenScape Office HX auf OpenScape Business V3 mit V3-Mainboard zu übertragen.

25.7.3 Migration eines HiPath 3000 Systems mit OpenScape Office V3 HX auf OpenScape Business V3 mit UC Booster Server

Die Migration muss in zwei Schritten erfolgen. In einem ersten Schritt werden die Systeme auf V2 migriert. In einem weiteren Schritt werden die Systeme auf V3 migriert.

Dieses Migrationsszenario sollte nur durchgeführt werden, wenn Kundendaten innerhalb des OpenScape Office HX-Servers beibehalten werden müssen. Die Migration ist zeitaufwändig und es muss ein neuer UC Booster Server eingerichtet werden. Die Migration endet mit einem OpenScape Business X V3 System mit V2-Mainboard und angeschlossenem UC Booster Server V3.

Eine Migration wie in [Migration eines HiPath 3000 Systems mit OpenScape Office V3 HX auf OpenScape Business V3 mit V3-Mainboard](#) auf Seite 807 sollte alternativ in Betracht gezogen werden, wenn die Kundendaten auf dem HX-Server nicht beibehalten werden müssen.

Schritt 1 Migration eines HiPath 3000 Systems mit OpenScape Office V3 HX auf OpenScape Business V2

Bei diesem Schritt wird HiPath 3000 nach OpenScape Business V2 migriert und die UC-Funktionalität des OpenScape Office V3 HX wird auf einen OpenScape Business UC Booster Server V2 gemappt.

Der UC Booster Server muss auf einer neuen HW- und SW-Basis vollkommen neu aufgesetzt werden. Die Lizenzen und Kundendaten können von OpenScape Office V3 HX auf den UC Booster Server übertragen werden, wenn der UC Booster Server zuerst mit der OpenScape Business SW-Version 1R2.2 eingerichtet wird. Nur in diesem Fall werden die folgende UC-Konfiguration sowie die Benutzerdaten übertragen:

- Ansagen
- Bilder
- Voicemail
- 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

Nach der Übertragung der Lizenzen und Kundendaten muss die UC Booster Server SW auf die SW-Version V1R3.3 und anschließend wieder auf die neueste SW-Version V2R7 aktualisiert werden.

Führen Sie für die Migration/Aktualisierung die folgenden 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 aktualisieren

Rüsten Sie falls noch nicht geschehen die OpenScape Office V3 HX auf die Software V3 R3FR6 hoch.

3) 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.

4) HiPath 3000 aktualisieren

Führen Sie die Aktualisierung von HiPath 3000 auf OpenScape Business V1 wie in der Migrationsprozedur für ein Standalone-System beschrieben durch (siehe [Migration von HiPath 33xx, 35xx, 3800 nach OpenScape Business X3/X5/X8 V3](#) auf Seite 793). 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.

5) UC Booster Server einrichten und in das Kunden-LAN integrieren

Das Linux-Betriebssystem SLES 64-Bit muss auf dem neuen Server-PC (Linux-Server) installiert werden, gefolgt von der Kommunikationssoftware (Version V1 R2.2). Details siehe *OpenScape Business Linux-Server Installationsanleitung*.

6) UC Booster aktivieren

Aktivieren Sie die UC Booster-Funktionalität im WBM des OpenScape Business Kommunikationssystems (**Grundinstallation > Erstinstallation > Paket mit UC Suite auf OpenScape Business UC Booster Server**) und geben Sie die IP-Adresse des neuen Server-PCs ein (mit der gleichen IP-Adresse wie der alte Server-PC, wenn möglich). 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](#).

7) 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](#) auf Seite 141.

8) 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.

Weitere Information dazu finden Sie in diesem Kapitel unter [Wie Sie ein OpenScape Office V3 HX Backup-Set konvertieren](#) auf Seite 811.

9) Aktualisierung der UC Booster Server Software auf V2

Aktualisieren Sie den UC Booster Server zuerst auf die Version V1 R3.3 und anschließend auf die neueste OpenScape Business V2 Software.

25.7.3.1 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>
```

```
/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.

25.7.4 Migration von HiPath 3000 Netzwerk auf OpenScape Business Netzwerk

Um ein HiPath 3000 Netzwerk auf ein OpenScape Business Netzwerk zu aktualisieren, sind die nachstehend beschriebenen Migrationsschritte durchzuführen.

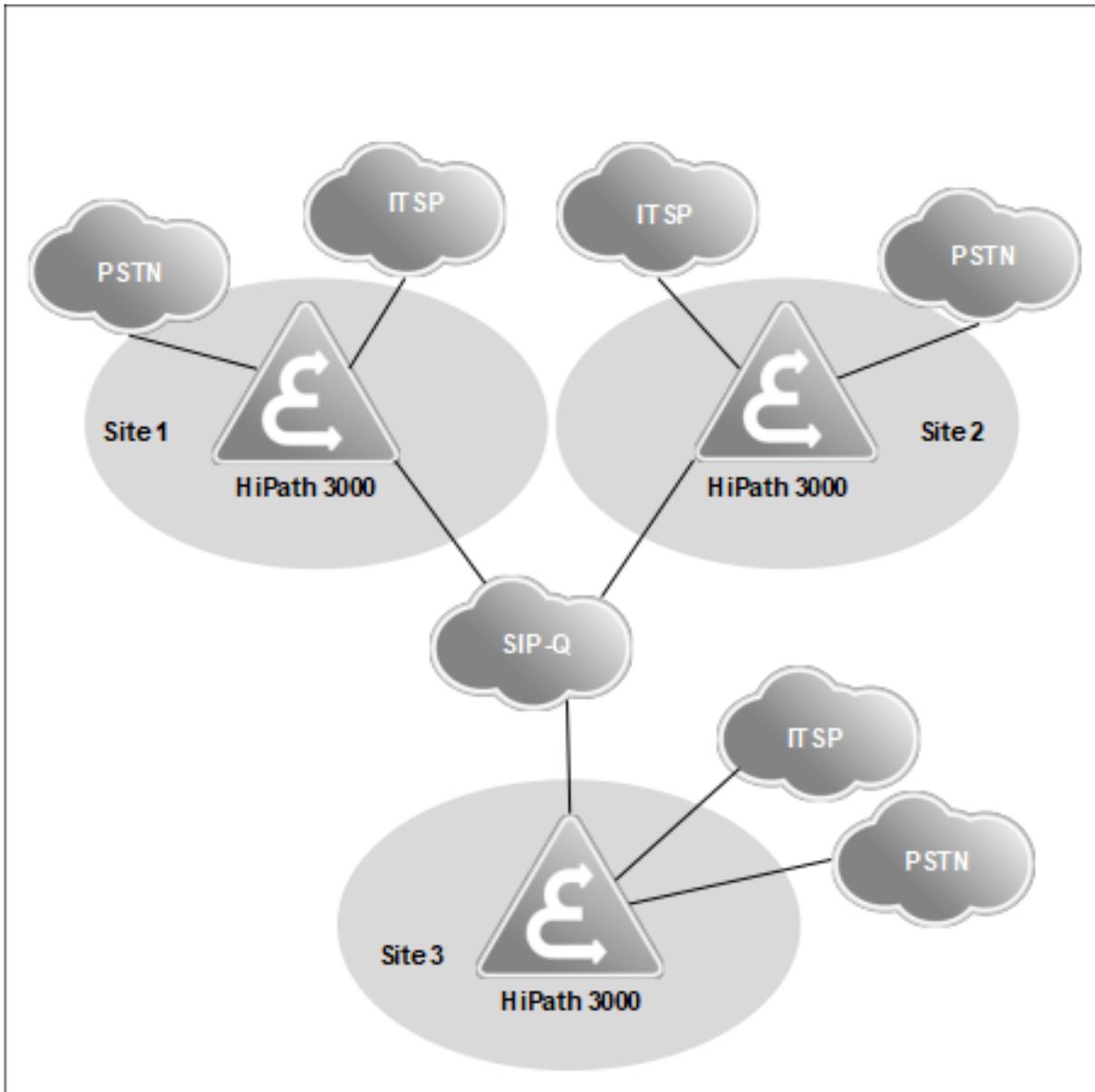


Abbildung 16: HiPath 3000 V9 Netzverbund

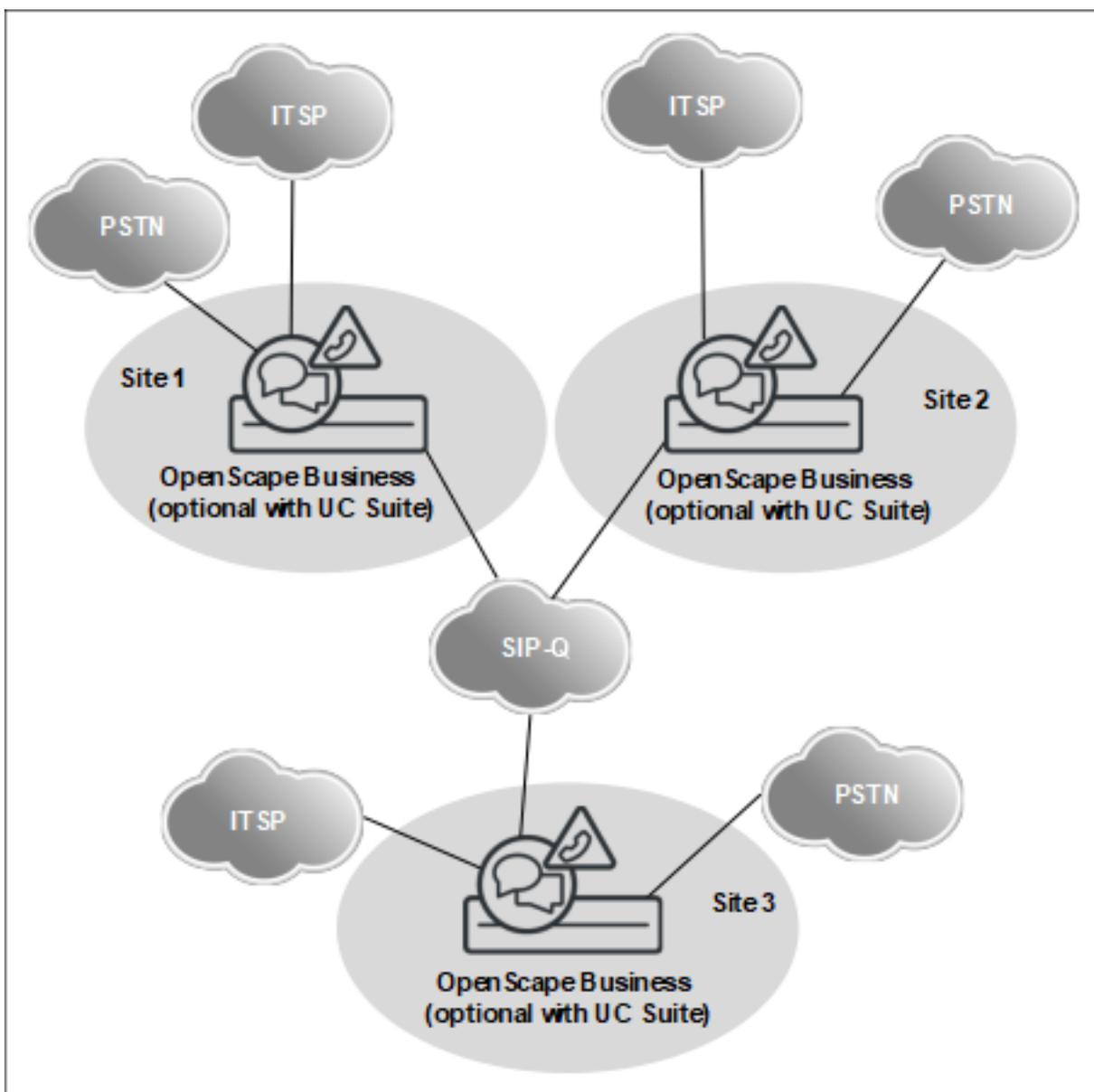


Abbildung 17: OpenScape Business Netzverbund

Migrationsschritte

Führen Sie folgende Schritte der Reihe nach durch:

1) HiPath 3000 aktualisieren

Alle HiPath 3000 Systeme des Netzverbunds sind separat gemäß der Migrationsbeschreibung eines Standalone-Systems zu aktualisieren (siehe 1.7.1).

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.

25.7.5 Migration eines HiPath 3000 V9 Netzverbands mit HiPath 5000 RSM

Ein HiPath 3000/5000 Netzwerk mit einer gemeinsamen Netzwerklizenzdatei kann über den zentralen Lizenzserver (CLS) in Standalone-Systeme mit einzelnen Lizenzdateien unterteilt werden. Jedes Standalone-System wird dann auf OpenScape Business migriert und separat lizenziert.

Bei Bedarf können die OpenScape Business Systeme nach der Migration am CLS wieder zu einer Netzwerkgruppe mit einer einzigen Netzwerklizenzdatei zusammengeführt werden.

Der Leistungsumfang von HiPath 5000 RSM wurde in OpenScape Business integriert, somit wird HiPath 5000 RSM selbst im OpenScape Business Netzwerk nicht mehr benötigt.

Für die Vernetzung der OpenScape Business Systeme sind zusätzlich OpenScape Business Networking-Lizenzen pro Knoten verfügbar.

Für Internettelefonie und T1-Leitungen sind zusätzliche Leitungslizenzen erforderlich.

Die folgenden Migrationsschritte müssen wie unten beschrieben ausgeführt werden.

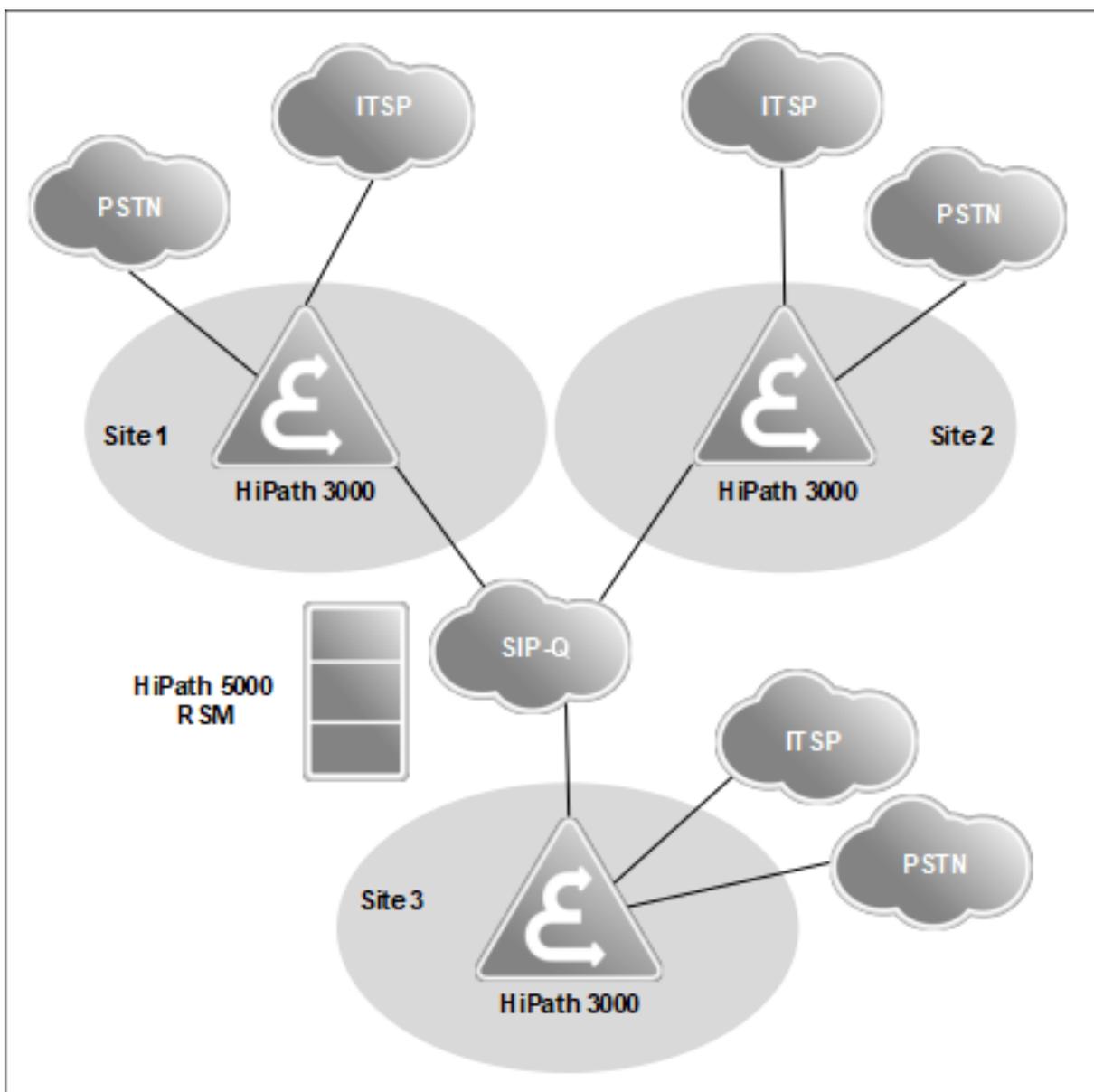


Abbildung 18: HiPath 3000 V9 Netzverbund

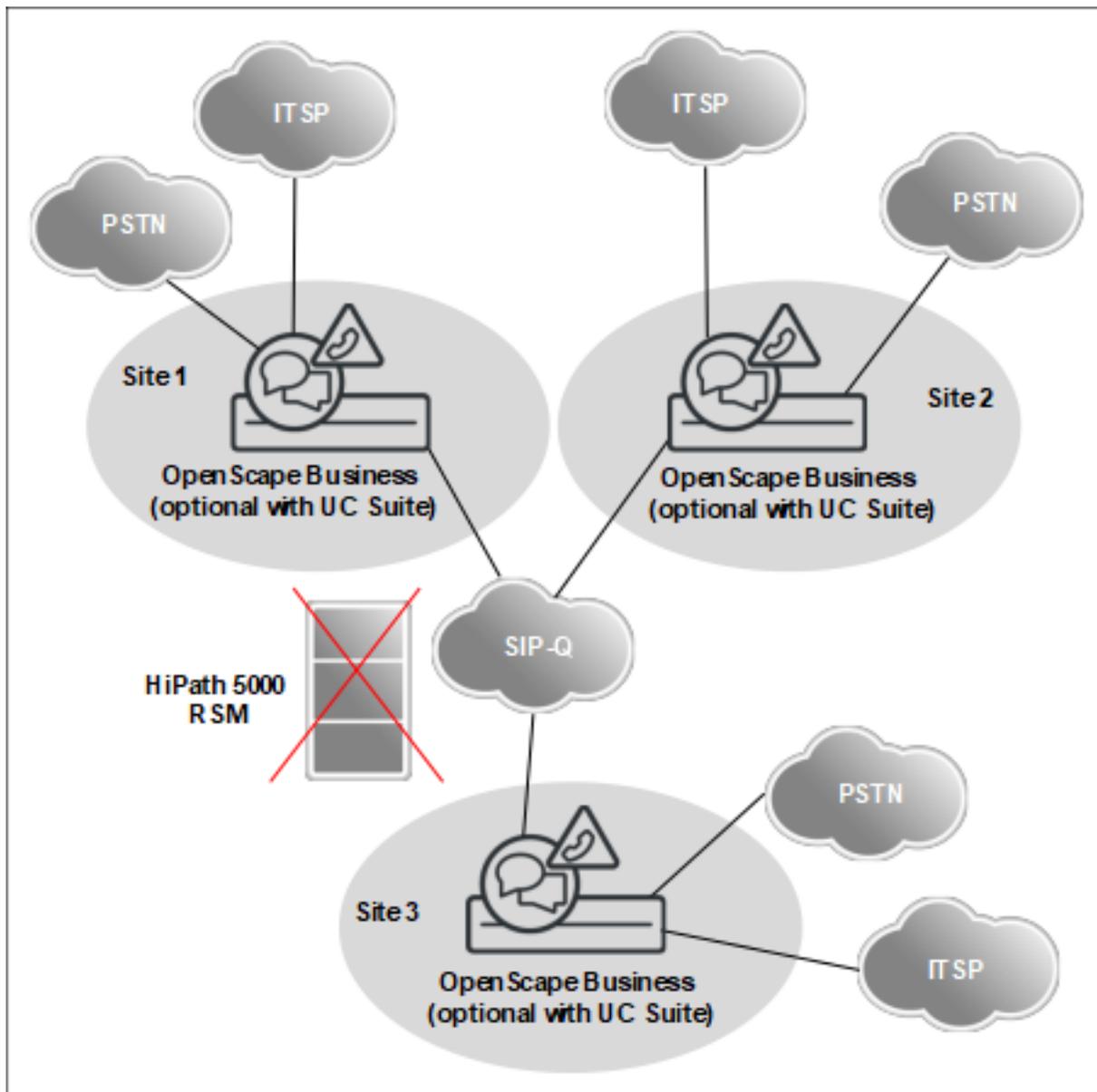


Abbildung 19: OpenScape Business Netzwerk

Migrationsschritte

Führen Sie folgende Schritte der Reihe nach durch:

1) Netzweite Lizenzierung auflösen

Ein HiPath 3000 Netzwerk mit HiPath 5000 RSM nutzt die netzweite Lizenzierung. Die Netzwerklicenzdatei 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 Netzwerkes 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 aktualisieren

Alle HiPath 3000 Systeme des Netzverbands sind separat gemäß der Migrationsbeschreibung eines Standalone-Systems hochzurüsten. Siehe 1.7.1

4) Konfiguration anpassen

Folgende Konfigurationsparameter sind nachträglich innerhalb von OpenScape Business über den WBM-Experten-Modus anzupassen:

- LCR-Einträge
- Voicemail-System (Sammelanschluss, Kennzahl zur Anwahl der Voicemail)
- Ansagen

5) Lizenzierung durchführen.

Nachdem alle Systeme aktualisiert sind, erfolgt die Zusammenfassung der einzelnen Lizenz-Dateien von OpenScape Business zu einer netzweiten Lizenz am CLS.

Anmerkung: Bei erweiterter netzweiter UC-Funktionalität ist eine Umstellung von offener auf verdeckte (geschlossene) Nummerierung erforderlich, um die internen Rufnummern anzupassen. Hierzu muss die offene Nummerierung deaktiviert werden, um anschließend die Knotennummer zu löschen und als Präfix neu hinzuzufügen (beispielsweise als erweiterte Internrufnummer 87100 statt 100 und 88100 statt 100).

Unterschiede:

- Die Auswahl der Teilnehmer auf ihrem eigenen Knoten erfolgt über die erweiterte Internrufnummer.
 - Die interne und die DuWa-Rufnummer dürfen voneinander abweichen, die Durchwahlnummern dürfen jedoch nicht geändert werden.
-

25.7.6 Geänderte/gestrichene Leistungsmerkmale und Schnittstellen von HiPath 3000

Einige HiPath 3000 Leistungsmerkmale und Schnittstellen sind für OpenScape Business in ihrer Funktion angepasst und erweitert worden.

Tausch der MMC-Karte

Der Austausch der SDHC-/M.2 SATA SSD-Karte bei eingeschaltetem System (bei HiPath 3000 als Speed-Update bekannt) ist aus technischen Gründen nicht möglich. Ferner kann die SDHC-/M.2 SATA SSD-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. Wenn die SDHC-/M.2 SATA SSD-Karte im System B verwendet werden soll, muss sie zunächst mit neuer Software initialisiert werden – mit Hilfe des Card Manager.

HG1500 DSP-Kanäle/B-Kanäle

Das HG1500-Modul wird nicht mehr benötigt. Die DSP-Funktionalität ist in OpenScape Business auf dem V3 Motherboard und über die optionalen Voice Channel Booster Cards integriert.

Bitte ermitteln Sie die Anzahl der benötigten DSP-Kanäle. DSP-Kanäle werden benötigt, um Netzübergänge von TDM-Telefonie auf VoIP zu realisieren. OpenScape Business hat auf dem V3-Mainboard 8 DSP-Kanäle integriert. Zur Erweiterung von DSP-Kanälen kann das DSP-Modul OCCB1/OCCBL (bis zu 40 Kanäle) oder das DSP-Modul OCCB3/OCCBH (bis zu 120 Kanäle) eingesetzt werden.

entry Web Services

Die entry Web Services werden nicht mehr unterstützt. Der Nachfolger von myPortal entry nennt sich myPortal @work und bietet einen erweiterten Funktionsumfang. myPortal for Mobile wird durch myPortal to go (Web Edition) ersetzt. Für den Einsatz von myPortal to go (Web Edition) ist der Plug PC nicht mehr nötig.

Entry Voicemail

Das Modul Entry Voicemail wird in OpenScape Business gestrichen. Die Funktion ist als Smart Voicemail in das OpenScape Business-Mainboard integriert. Smart Voicemail-Benutzer müssen lizenziert werden.

Externe Voicemail

Wird bei HiPath 3000 eine externe Voicemail-Lösung wie z. B. Xpressions verwendet, müssen nach der KDS-Konvertierung die 10 EVM-Ports im Manager E von **Phonemail** auf **Standard** gesetzt 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)

SIP-Trunking

Zur Anbindung externer SIP-Server (z.B. OpenScape Alarm Server, HiPath 4000, OpenScape Voice oder UC-Suite) stehen in OpenScape Business zusätzliche native SIP-Q-Richtungen zur Verfügung (bei HiPath 3000 nur eine SIP-Q-Richtung). Damit sind zusätzlich zu den klassischen Richtungen für Amt, Vernetzung und ITSP, native SIP/SIP-Q-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).

Anmerkung: Vereinfachtes Wählen wird in CSTA-Anwendungen nicht unterstützt.

VoIP over PPP via ISDN

Geroutete Sprachverbindungen über Leitungen mit geringer Bandbreite werden nicht mehr unterstützt

G.723-Unterstützung

G.723-Codexs werden nicht mehr unterstützt.

Raumüberwachung (Babyphone)

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.

HiPath 3000 BS4

Lizenzen für Basisstationen werden in OpenScape Business nicht mehr benötigt.

SSDP auf Basis des Plug PC

SSDP ist in OpenScape Business integriert. Der Plug PC ist nicht mehr nötig.

Accounting-Schnittstelle

Die Schnittstellen der Accounting-Daten sind gegenüber HiPath 3000 geändert.

V24-Applikationen

V24-Applikationen werden nicht mehr unterstützt.

CSTA-Applikationen

Innerhalb von OpenScape Business V3 ist entweder ein V3-Mainboard oder UC Booster Card / Server in Kombination mit einem V2-Mainboard für die Verbindung von CSTA-Applikationen erforderlich. In einem Netzverbund dürfen V3-Mainboard / UC Booster Card / Server nur auf dem Master-Knoten vorhanden sein. Die Applikationen müssen CSTAv3-Protokoll unterstützen. Im Vergleich zu HiPath 3000 wurden Änderungen am CSTA-Protokoll implementiert. Daher sind CSTA-Applikationen am HiPath 3000 V9 ggf. nicht kompatibel einsetzbar bei OpenScape Business. Das CSTAv2-Protokoll wird nicht mehr unterstützt.

In SW-Version 3 ist eine CSTA-Lizenz für die Verwendung der CSTA-Schnittstelle mit folgenden Ausnahmen erforderlich:

- UC Booster Card CSTA-Verbindungen im Allgemeinen
- OpenScape Business TAPI 120 oder TAPI 170 CSTA-Verbindungen im Allgemeinen

Für die OpenScape Business CSTA-Schnittstelle gelten im Vergleich zur HiPath 3000 CSTA-Schnittstelle die nachfolgend beschriebenen Änderungen.

- Die Anschaltung an die CSTA-Schnittstelle ist für einzelne und vernetzte OpenScape Business Slave-Knoten identisch. CSTA auf dem Master-Knoten in einem Netzwerk bietet erweiterte Funktionen. Sie erfolgt ausschliesslich über LAN. RS232 (V.24) und S0 Schnittstellen werden nicht mehr unterstützt.
- Hard- und Software-Zusatzkomponenten wie CSTA Service Provider (CSP), HG 1500 Baugruppe oder HiPath 5000 RSM System werden bei OpenScape Business nicht mehr benötigt. Stattdessen werden UC Booster HW oder V3-Mainboards benötigt.

- Die CSTA-Schnittstelle ist mit Ausnahme von UC Booster Card- und TAPI 120/170-Verbindungen lizenziert.
- Maximal 4 CSTA-Links können zur Anschaltung externer Applikationen verwendet werden. Im Auslieferungszustand sind 3 der 4 CSTA Schnittstellen zur Verwendung von internen Applikationen von OpenScape Business vorkonfiguriert. Diese können optional auch zur Anschaltung externer Applikationen eingesetzt werden.
- Die Absicherung der CSTA Schnittstellen gegen Missbrauch wurde verbessert. Der Zugangsmechanismus wurde überarbeitet.
- MULAP-Monitoring über CSTA ist nur möglich, wenn ein Monitorpunkt auf die MULAP-Nummer gesetzt wird. Einzelne MULAP-Mitglieder können nicht überwacht werden. Möchte eine CSTA-Applikation dennoch einzelne MULAP-Mitglieder überwachen, werden von OpenScape Business keine CSTA-Events an die Applikation übertragen. Das gilt auch für MULAP-Mitglieder, die Teil eines Sammelanschlusses sind.
- Die zur Verfügung gestellten CSTA-Funktionen wurde erweitert. Details sind im OpenScape Business CSTA Interface Manual beschrieben.
- Die CSTA Phase II Protokollversion wird nicht mehr unterstützt.
- CSTA-Applikationen, die an OpenScape Business betrieben werden, sollten in Verbindung mit OpenScape Business getestet und freigegeben sein.

HiPath TAPI 120/170 V2-Anwendungen

Für HiPath TAPI 120/170 V2 können die bestehenden Lizenzen nicht übernommen werden. Es müssen neue Lizenzen gekauft werden. HiPath 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-Benutzer erforderlich (damit ist auch TAPI120 für die ersten 6 Benutzer nicht mehr lizenzfrei). Der CMD (CSTA Message Dispatcher) ist in OpenScape Business integriert. Ein separater Windows-Server für den CMD ist daher nicht mehr erforderlich. Die Anbindung an externe TAPI-Anwendungen ist für OpenScape Business und OpenScape Business S möglich. OpenScape Business erfordert ein V3-Mainboard oder UC Booster Card / Server. In einem Netzverbund muss entweder OpenScape Business S vorhanden sein oder ein V3-Mainboard, eine UC Booster Card oder ein UC Booster Server muss zumindest auf dem Master-Knoten vorhanden sein.

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.

Migration

- 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.

Weitere externe Applikationen

Nachrangige Anwendungen, die extern an HiPath 3000 angebunden sind, können auf OpenScape Business nicht mehr betrieben werden.

HiPath 3000 Application	Nachfolgeanwendung für OpenScape Business	Hinweise
optiClient Attendant	OpenScape Business Attendant	Neue Anwendung Keine Lizenzübertragung möglich
optiClient BLF V1/V2	OpenScape Business Attendant (OpenScape Business BLF)	Neue Anwendung Keine Lizenzübertragung möglich
HiPath TAPI 120/170	OpenScape Business TAPI 120/170	Neue Anwendung Keine Lizenzübertragung möglich
Communication Clients der Entry WEB Services auf Plug PC	Integrierte UC-Lösung	Neue Anwendung Keine Lizenzübertragung möglich
myPortal for Mobile/ Tablet	myPortal to go	Neue Anwendung Keine Lizenzübertragung möglich

Geänderte/gestrichene Leistungsmerkmale von HiPath 5000 RSM

HiPath 5000 RSM wird nicht mehr unterstützt. Die Funktionalität von HiPath 5000 RSM wurde in OpenScape Business integriert. Das bedeutet, dass kein separater Server mehr benötigt wird.

Tabelle 37: Unterschiede zwischen HiPath 5000 RSM und OpenScape Business V3

Leistungsmerkmal	HiPath 5000 RSM	OpenScape Business
netzweite Lizenzierung, Zuordnung der Lizenzen zu den einzelnen Knoten	Alle System-Lizenzen des Netzes sind am CLS zu einer netzweiten Lizenz zusammengefasst.	Alle System-Lizenzen des Netzes sind 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. Das Nummerierungsschema wird über das Netzwerk synchronisiert.	Über OpenScape Business Assistant (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 10 SIP-Interconnection-Richtungen mit bis zu 2 SIP-Q bzw. 10 Native SIP oder bis zu 8 ITSP
Resilience / Survivability	User-Survivability für HFA-Telefone bei geschlossener Nummerierung	User-Survivability für HFA-Telefone mit geschlossener Nummerierung (Wechsel von OpenScape Business S <-> OpenScape Business X3 / X5 / X8)
Backup / Restore	Netzweit	Lokal
Inventory-Funktion	Netzweit	Lokal

Migration

Leistungsmerkmal	HiPath 5000 RSM	OpenScape Business
Presence Manager	netzweite Funktion mit der Bereitstellung von 5000 RSM	Netzwerkweite Funktion durch Bereitstellung eines Multi-Node CSP basierend auf der OpenScape Business UC Booster Card, dem OpenScape Business UC Booster Server oder OpenScape Business S. Voraussetzung: geschlossene Nummerierung.
TAPI 170 am Standalone-System	TAPI 170 am Standalone-System läuft auf einem Windows-PC mit eigener Lizenzierung (separate Lizenzdatei 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 OpenScape Business. Die Anbindung des TAPI 170 erfolgt über den CSP des Systems (OpenScape Business UC Booster Card, OpenScape Business UC Server Booster oder OpenScape Business S).
TAPI 170 im Netzverbund	TAPI 170 läuft auf 5000 RSM mit eigener Lizenzierung (separate Lizenzdatei 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 Multinode-CSP des Master-Knotens (d.h. netzweit). Voraussetzung: geschlossene Nummerierung

Gemischte Netze

Ein gemischter Netzverbund aus OpenScape Business und OpenScape Office wird nicht unterstützt.

25.8 Migration innerhalb von OpenScape Business V3

Beschrieben werden die verschiedenen Migrationsmöglichkeiten innerhalb von OpenScape Business X V3 Systemen mit V2-Mainboards.

Anmerkung: Diese Szenarien sind für OpenScape Business X V3 Systeme mit V3-Mainboards überholt (nicht gültig)!

Erhöhung der Anzahl von UC Smart Benutzern

Es gibt folgende Möglichkeiten:

- Migration von **OpenScape Business X** (UC Smart) auf **OpenScape Business X** mit **UC Booster Card** (UC Smart)
Sinnvoll für 50 - 150 UC Smart Benutzer. Alle Konfiguration- und Benutzerdaten werden übernommen. Bei Downgrades findet keine Datenübertragung statt. Für die neuen UC-Smart-Benutzer sind zusätzliche UC-Benutzerlizenzen erforderlich. OpenScape Business X1 ist nicht mit der UC Booster Card erweiterbar.
- Migration von **OpenScape Business X** (UC Smart) auf **OpenScape Business X** mit **UC Booster Server** (UC Smart)
Sinnvoll für 50 - 500 UC Smart Benutzer. Alle Konfiguration- und Benutzerdaten werden übernommen. Bei Downgrades findet keine Datenübertragung statt. Für die neuen UC-Smart-Benutzer sind zusätzliche UC-Benutzerlizenzen erforderlich.
- Migration von **OpenScape Business X** mit **UC Booster Card** (UC Smart) auf **OpenScape Business X** mit **UC Booster Server** (UC Smart)
Sinnvoll für 150 - 500 UC Smart Benutzer. Alle Konfiguration- und Benutzerdaten werden übernommen. Bei Downgrades findet keine Datenübertragung statt. Für die neuen UC-Smart-Benutzer sind zusätzliche UC-Benutzerlizenzen erforderlich.

Upgrade von UC Smart auf UC Suite

Es gibt folgende Möglichkeiten:

- Migration von **OpenScape Business X** (UC Smart) auf **OpenScape Business X** mit **UC Booster Card** (UC Suite)
Die Konfiguration- und Benutzerdaten werden nicht übernommen. Für vorhandene UC Smart Clients ist eine Upgradelizenz auf UC Suite Clients nötig. Die Umstellung der UC-Lösung auf UC Suite erfolgt im WBM mit dem Wizard **Erstinstallation**.
- Migration von **OpenScape Business X** (UC Smart) auf **OpenScape Business X** mit **UC Booster Server** (UC Suite)
Die Konfiguration- und Benutzerdaten werden nicht übernommen. Für vorhandene UC Smart Clients ist eine Upgradelizenz auf UC Suite Clients nötig. Die Umstellung der UC-Lösung auf UC Suite erfolgt im WBM mit dem Wizard **Erstinstallation**.

Migration

Migration von HW-Baugruppen

- Migration von **OpenScape Business X** mit **UC Booster Card** (UC Smart) auf **OpenScape Business X** mit **UC Booster Server** (UC Suite)

Die Konfiguration- und Benutzerdaten werden nicht übernommen. Für vorhandene UC Smart Clients ist eine Upgradelizenz auf UC Suite Clients nötig. Die Umstellung der UC-Lösung auf UC Suite erfolgt im WBM mit dem Wizard **Erstinstallation**.

- Migration innerhalb **OpenScape Business S** von UC Smart auf UC Suite

Die Konfiguration- und Benutzerdaten werden nicht übernommen. Für vorhandene UC Smart Clients ist eine Upgradelizenz auf UC Suite Clients nötig. Die Umstellung der UC-Lösung auf UC Suite erfolgt im WBM mit dem Wizard **Erstinstallation**.

- Migration innerhalb **OpenScape Business UC Booster Server** von UC Smart auf UC Suite

Die Konfiguration- und Benutzerdaten werden nicht übernommen. Für vorhandene UC Smart Clients ist eine Upgradelizenz auf UC Suite Clients nötig. Die Umstellung der UC-Lösung auf UC Suite erfolgt im WBM mit dem Wizard **Erstinstallation**.

Erhöhung der Anzahl von UC Suite Benutzern

Es gibt folgende Möglichkeiten:

- Migration von **OpenScape Business X** mit **UC Booster Card** (UC Suite) auf **OpenScape Business X** mit **UC Booster Server** (UC Suite)

Sinnvoll für 150 - 500 UC Suite Benutzer. Alle Konfiguration- und Benutzerdaten werden übernommen. Bei Downgrades findet keine Datenübertragung statt. Für die neuen UC Suite-Benutzer sind zusätzliche UC-Benutzer- oder Groupware-Benutzerlizenzen erforderlich.

25.9 Migration von HW-Baugruppen

Die folgenden Aktionen zur Hardware-Migration sind für ein OpenScape Business X8-System möglich:

- Ersetzen von SLMO24N durch SLMU
- Ersetzen von SLMO8N durch SLMU
- Ersetzen von SLCN durch SLMUC (SLMU + CMAe)

25.9.1 Ersetzen von SLMO24N durch SLMU

Ein einfacher Kartenaustausch wird unterstützt. Die SLMO24N kann aus dem System entfernt und die neue SLMU eingesteckt werden. Alle konfigurierten Ports bleiben unverändert. Das Ausschalten des Systems ist nicht erforderlich.

25.9.2 Ersetzen von SLM8N durch SLMU

Da die SLMU-Karte mehr Ports als die SLMO8 besitzt, muss diese über die Administration entfernt werden. Um die Karte aus dem System zu entfernen, sollte der Online-Benutzer mit folgendem Dialog verwendet werden:

Systemadministration 29- 4 - 1

und ändern Sie den Kartentyp zu SLMUC.

Anmerkung:

Wenn die Benutzer für UC Suite konfiguriert sind, werden sie mit den Standardeinstellungen erstellt. Alle vorherigen Daten (z. B. Sprachbox, Fax, Benutzereinstellungen) gehen verloren.

Anmerkung:

Wenn die SLMO8- durch die SLMU-Karte ersetzt wird, ohne die Karte anhand der beschriebenen Schritte zu entfernen, könnten die zusätzlichen 16 Ports der SLMU-Karte nicht funktionsfähig sein, da sie nicht konfiguriert werden konnten. Dies geschieht, wenn bereits eine andere Karte den Port-Bereich dieser 16 Ports verwendet. Wenn nur eine SLMO8 im System vorhanden ist, sind bei einem Austausch durch die SLMU-Karte alle Ports verfügbar.

25.9.3 Ersetzen von SLCN durch SLMUC (SLMU + CMAe)

Da die SLMU-Karte mehr Ports als die SLCN besitzt, muss diese über die Administration entfernt werden, bevor die SLMUC an diesem Steckplatz eingesetzt wird. Die Schritte zur Entfernung der Karte sind folgende:

- 1) Aufheben der Registrierung aller CMI-Mobilteile an ihrer Basisstation**
- 2) Entfernen Sie die Karte aus dem System.**
- 3) Entfernen Sie die SLCN-Karte über den Online-Benutzer mit dem Dialog:**

Systemadministration 29- 4 - 1

und ändern Sie den Kartentyp zu SLMUC.

- 4) Installation der SLMUC-Karte**
- 5) Konfigurieren des verwendeten Mobilteils**
- 6) Registrieren der CMI-Mobilteile**

Alle Benutzer der betroffenen DECT-Telefone (maximal 128) müssen diese zur Neuregistrierung abgeben.

Anmerkung:

Migration

Migration von OpenScape Business X1 V2 auf OpenScape Business X1W V3

Beim Ersetzen einer SLCN-Karte durch eine SLMUC ist auch eine Blindblende statt der für die SLCN verwendeten Kunststoffblende erforderlich.

Anmerkung:

Wenn die Benutzer für UC Suite konfiguriert sind, werden sie mit den Standardeinstellungen erstellt. Alle vorherigen Daten (z. B. Sprachbox, Fax, Benutzereinstellungen) gehen verloren.

25.10 Migration von OpenScape Business X1 V2 auf OpenScape Business X1W V3

Bei der Migration eines OpenScape Business X1-Modells muss das gesamte System ausgetauscht werden.

Bestehende Lizenzen können übernommen werden. Die Kundenkonfiguration kann nicht übernommen werden und muss nach der Migration manuell wiederhergestellt werden. Der bestehende Software-Support wird nach der Migration unverändert weitergeführt oder es wird ein neues Software-Support-Datum für das V3-Mainboard übernommen, wenn dieses über den 31.12.2026 hinaus gültig ist.

Vor der Migration sollte im System ein permanenter Zugang zum Unify-Lizenzserver (über das Internet) eingerichtet werden, falls nicht bereits vorhanden, und die Funktion „CLS Connect“ sollte aktiviert werden. Das vereinfacht die Lizenzübertragung und verkürzt erheblich die Migrationszeit. Der Kunde muss über den erforderlichen Zugang vom OpenScape Business System zum CLS informiert werden.

Erforderliche Bestellpositionen

Für die Migration des Modells X1 auf X1W mit V3-Mainboard ist Folgendes erforderlich, je nachdem, ob CLS Connect, UC Suite oder externe CSTA-Applikationen verwendet werden:

- X1W-System
- V3 SW auf M.2 SATA SSD-Datenspeicher
- M2 SSD 256 GB Massenspeicher (optional mit Applikation UC Suite)
- OpenScape Business Upgrade für OS Biz X1-Lizenz (wird immer benötigt)
- OpenScape Business CSTA-Lizenz (optional)

Bedingungen für funktionale Grenzen

Im Verlauf der Migration können bestehende Lizenzen vom vorhandenen X1-System vollständig auf das X1W-System mit V3 Mainboard übertragen werden. Die Lizenzübertragung ohne Aktivierung der Funktion CLS Connect erfordert die Lizenz „Migration“ und eine viel komplexere Handhabung und mehr Zeitaufwand als die Verwendung der Funktion CLS Connect.

X1-Systeme mit aktivem CLS Connect können nicht über die Funktion „Regeneration“ zu X1W-Systemen mit V3-Mainboard aufgerüstet werden. Die Lizenz „OpenScape Business Upgrade für OS Biz X1“ muss immer aktiviert werden, aber es muss kein Bestätigungscode während des Upgrade-Prozesses eingegeben werden.

Ein Upgrade von OpenScape Business X1 PAYGO-Systemen auf OpenScape Business X1W PAYGO-Systeme wird nicht unterstützt.

Für den Fall, dass OpenScape Personal Edition-Clients auf dem System betrieben werden und entsprechende Lizenzen vorhanden sind, müssen diese immer manuell am zentralen Lizenzserver für die neue Locking-ID (MAC-Adresse) des V3-Mainboards neu generiert werden, unabhängig davon, ob CLS Connect verwendet wird oder nicht.

Die Kundenkonfiguration kann nicht übernommen werden und muss nach der Migration manuell wiederhergestellt werden.

Technische Abwicklung der Migration

Die wichtigsten technischen Schritte der Migration werden nachfolgend beschrieben. Es wird unterschieden zwischen

- Migration mit permanenter Lizenzierung
 - Migration mit aktivierter CLS Connect-Funktion und Anbindung an den zentralen Lizenzserver
 - Migration ohne CLS Connect-Funktion und ohne Anbindung an den zentralen Lizenzserver

Weitere Details zur technischen Abwicklung der Migration finden Sie im Handbuch OpenScape Business Administrations.

25.10.1 Wie Sie permanent lizenzierte Systeme mit CLS Connect auf X1W V3 migrieren

Schritt für Schritt

- 1.** Generieren Sie die Lizenzdateien auf dem zentralen Lizenzserver (CLS).
 - a) Aktivieren Sie die Lizenz „OpenScape Business Upgrade für OS Biz X1“ auf dem X1-System mit V2-Mainboard. Geben Sie während des Aktivierungsvorgangs die MAC-Adresse des V3-Mainboards an.
 - b) Generieren Sie eine neue Lizenzdatei für die MAC-Adresse auf dem X1W-System mit V3-Mainboard. Diese Lizenzdatei enthält die erweiterte SW-Unterstützung.
 - c) Übertragung eventuell vorhandener Personal Edition-Lizenzen von der MAC-Adresse des V2-Mainboards auf die MAC-Adresse des V3-Mainboards mittels der Funktion „Regenerieren“ und Generierung einer neuen Lizenzdatei für die Personal Edition-Lizenzen.
- 2.** Bereiten Sie das OpenScape Business System vor.
 - a) Aktualisieren Sie das vorhandene System auf SW-Version V2R7.

- b) Richten Sie im System einen Zugang zum zentralen Lizenzserver (Central License Server, CLS) ein und testen Sie die Verbindung.
 - c) Aktivieren Sie CLS Connect im System. Falls noch nicht geschehen, wird der SW-Support erneut um 3 Monate verlängert.
- 3. X1-Systemwechsel**
- a) Fahren Sie das X1-System herunter und schalten Sie alle Versorgungsspannungen aus.
 - b) Verwenden Sie V3-Datenträger und ggf. optionale Massenspeicher auf dem X1W-System.
 - c) Entfernen Sie die CAME- und/oder die OCCB Voice Channel Booster-Karte vom V2-Mainboard und stecken Sie sie in das X1W V3-Mainboard ein.
 - d) Ersetzen Sie das X1-System durch das X1W-System.
 - e) Schließen Sie das Erdungskabel an das X1W-System an.
 - f) Schließen Sie die Telefon-, Amtsleitungs-, LAN- und ggf. USB-Kabel an das X1W-System an.
 - g) Versorgungsspannungen wieder einschalten, System bootet automatisch.
- 4. Stellen Sie nach dem Hochfahren die grundlegenden Systemparameter in WBM ein.**
- a) Stellen Sie Systemdatum und -uhrzeit ein.
 - b) Stellen Sie das Applikationspaket ein.
 - UC Smart für Systeme ohne UC oder mit UC Smart
 - UC Suite für Systeme mit UC Suite
 - c) Stellen Sie die Systemkonfiguration wieder her.
 - Manuelle Konfiguration des X1W.
 - Importieren Sie die neu erstellte Lizenzdatei.

25.10.2 Wie Sie permanent lizenzierte Systeme ohne CLS Connect auf X1W V3 migrieren

Schritt für Schritt

- 1.** Bereiten Sie das OpenScape Business System vor.
 - a) Aktualisieren Sie das vorhandene System auf SW-Version V2R7.
- 2.** Erstellen Sie auf dem zentralen Lizenzserver (CLS) eine Migrationslizenzdatei für das X1 mit V2-Mainboard.
 - a) Aktivieren Sie die „X1-Migrationslizenz“ für das vorhandene System.
 - b) Generieren Sie die neue Lizenzdatei für die MAC-Adresse des V2-Mainboards. Dazu muss die MAC-Adresse des X1W-Systems auf dem CLS eingegeben werden.
 - c) Laden Sie die Lizenzdatei vom CLS herunter. Diese Lizenzdatei enthält die erweiterte SW-Unterstützung.

- 3.** Importieren Sie die Lizenzdatei in das OpenScape Business X1-System mit V2-Mainboard.
- 4.** Notieren Sie den Bestätigungscode, der im OpenScape Business Assistent angezeigt wird.
- 5.** Generieren Sie auf dem zentralen Lizenzserver (CLS) eine neue Lizenzdatei für das X1W-System mit V3-Mainboard.
 - a) Erstellen Sie auf dem CLS eine neue Lizenzdatei für die MAC-Adresse des X1W-Systems mit V3-Mainboard, indem Sie die MAC-Adresse des X1 mit V2-Mainboard mit dem zuvor notierten Bestätigungscode erneut generieren.
 - Suchen Sie auf dem CLS das OpenScape Business System mit der MAC-Adresse des X1W-Systems mit V3-Mainboard.
 - Entsperren Sie das OpenScape Business System, indem Sie den Bestätigungscode eingeben und aktivieren.
 - Generieren Sie die Lizenzdatei erneut.
 - b) Laden Sie die neu generierte Lizenz vom CLS herunter.
- 6.** Austausch des Mainboards
 - a) Fahren Sie das System herunter und schalten Sie alle Versorgungsspannungen aus.
 - b) Verwenden Sie V3-Datenträger und ggf. optionale Massenspeicher auf dem X1W-System mit V3-Mainboard.
 - c) Entfernen Sie die CAME- und/oder die OCCB Voice Channel Booster-Karte vom V2-Mainboard und stecken Sie sie in das X1W-System mit V3-Mainboard ein.
 - d) Ersetzen Sie das X1-System mit V2-Mainboard durch das X1W-System mit V3-Mainboard.
 - e) Schließen Sie das Erdungskabel an das X1W-System an.
 - f) Schließen Sie die Telefon-, Amtsleitungs-, LAN- und ggf. USB-Kabel an das X1W-System an.
 - g) Schalten Sie die Stromversorgung wieder ein und das System startet automatisch.
- 7.** Stellen Sie nach dem Hochfahren die grundlegenden Systemparameter in WBM ein.
 - a) Stellen Sie Systemdatum und -uhrzeit ein.
 - b) Stellen Sie das Applikationspaket ein.
 - UC Smart für Systeme ohne UC oder mit UC Smart
 - UC Suite für Systeme mit UC Suite
 - c) Stellen Sie die Systemkonfiguration wieder her.
 - Manuelle Konfiguration des X1W
 - d) Importieren Sie nach dem Hochfahren des Systems manuell die neue Lizenzdatei in das V3-System.

26 Ausbaugrenzen und Kapazitäten

Die Ausbaugrenzen und Kapazitäten basieren auf systembedingten Maximalwerten für ein Einzelsystem. Die Maximalwerte eines Systems in einem Netzwerk können unterschiedlich sein.

26.1 Maximalwerte für Teilnehmer

- Daten für Systeme mit V2 OCC Mainboards finden Sie in [Tabelle 38: Ausbaustufe Teilnehmer/Benutzer mit OCCx Mainboards](#) auf Seite 832
- Daten für Systeme mit V3 OCC Mainboards finden Sie in [Tabelle 39: Ausbaustufe Teilnehmer/Benutzer mit OCCSB/R, OCCMA/B oder OCCLA Mainboards](#) auf Seite 833
- Daten für OpenScape Business S Server-Systemen finden Sie in [Tabelle 40: Ausbaustufe Teilnehmer/Benutzer mit OpenScape Business S](#) auf Seite 835

Tabelle 38: Ausbaustufe Teilnehmer/Benutzer mit OCCx Mainboards

Teilnehmer	X1	X3W/R	X5W/R	X8
Teilnehmermaximum				
Max. Anzahl Teilnehmer ¹⁶	30	500	500	500
IP-Teilnehmer				
IP-Teilnehmersystem (HFA)	20 ¹⁷	500	500	500
IP-Teilnehmer (SIP)	20 ¹⁷	500	500	500
TDM-Teilnehmer				
Max. Anzahl der TDM-Teilnehmer ^{18 22}	30	384	384	384
Analoge Teilnehmer (TDM)	4	20	68	384
U _{P0} -Master-Teilnehmer (TDM) ²²	8	24	56	384
U _{P0} -Slave-Teilnehmer (TDM) (inkl. a/b- und S0-Adapter)	8	24	56	116
S0-ISDN-Teilnehmer (TDM)	2	36	52	128
DECT-CMI-Teilnehmer (TDM)	16	64	64	250
Mobility-Teilnehmer				
Max. Anzahl der Mobility-Teilnehmer ¹⁹	30	150	150	150
Mobility Entry-Teilnehmer	20	150	150	150
myPortal to go-Teilnehmer ²⁰	30	150	150	150

Teilnehmer	X1	X3W/R	X5W/R	X8
Circuit-Teilnehmer ²¹	30	150	150	150
Skype for Business-Teilnehmer	30	150	150	150
Andere Teilnehmer				
RAS-Teilnehmer	2	500	500	500
Virtuelle Teilnehmer frei konfigurierbar	30	250	250	250

Anmerkung: Für jede Systemkonfiguration muss geprüft werden, ob die Nennleistungsabgabe der systemeigenen Stromversorgung ausreicht oder ob eine externe Zusatzspeisung erforderlich ist (siehe *OpenScape Business Servicedokumentation - Leistungsbedarf eines Kommunikationssystems*).

Tabelle 39: Ausbaustufe Teilnehmer/Benutzer mit OCCSB/R, OCCMA/B oder OCCLA Mainboards

Teilnehmer	X1W		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Teilnehmer maximal								
Max. Anzahl Teilnehmer ¹⁶	30	30	500	500	500	500	500	500
IP-Teilnehmer								
IP-Teilnehmersystem (HFA)	500	500	500	500	500	500	500	500

¹⁵ Werte sind gestaffelt nach UC Booster-Konfiguration: Booster Server / Booster Card / ohne UC Booster

¹⁶ Summe von: Teilnehmer IP (HFA), IP (SIP), Analog, UP0 Master/Slave, DECT (CMI), ISDN S0, Mobility und Deskshare

¹⁷ Summe von IP-Benutzern und Desk Share-Benutzern (Beschränkung durch Konfiguration)

¹⁸ Summe von: Teilnehmer Analog, UP0, DECT (CMI) und ISDN S0

¹⁹ Summe von: Teilnehmer Mobility Entry, myPortal to go, Circuit, Skype for Business

²⁰ Die Anzahl der gleichzeitigen VoIP-Verbindungen der Teilnehmer hängt ab von:

1) den im System verfügbaren DSP-Kanälen für Gateway-Anrufe (IP/TDM-Übergang).

2) den im System verfügbaren internen RTP-Proxykanälen für VoIP-Anrufe über das Internet.

²¹ der Anzahl der gleichzeitigen Verbindung je nach den im System verfügbaren DSP-Kanälen für Gateway-Anrufe (IP/TDM-Übergang).

²² Abhängig von den Telefontypen und dem Gesamtleistungsbedarf des Kommunikationssystems

Ausbaugrenzen und Kapazitäten

Teilnehmer	X1W		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
IP-Teilnehmer (SIP)	500	500	500	500	500	500	500	500
TDM-Teilnehmer								
Max. Anzahl der TDM-Teilnehmer ¹⁸ 22	384	384	384	384	384	384	384	384
Analoge Teilnehmer (TDM)	4	4	20	20	68	68	384	384
U _{P0} Master/ Slave-Teilnehmer (TDM) ²²	8	8	24	24	56	56	384 Master 116 Slave	384 Master 116 Slave
S0-ISDN-Teilnehmer (TDM)	0	0	32	32	48	48	128	128
DECT-CMI-Teilnehmer (TDM)	16	16	64	64	64	64	250	250
Mobility-Teilnehmer								
Max. Anzahl der Mobility-Teilnehmer ¹⁹	150/ 500 ²³	500	500					
Mobility Entry-Teilnehmer	150	20	150	150	150	150	150	150
myPortal to go-Teilnehmer ²⁰	150/ 500 ²³	30	150/ 500 ²³	150/ 500 ²³	150/ 500 ²³	150/ 500 ²³	500	500
myPortal for Teams-Teilnehmer ²⁰	150/ 500 ²³	30	150/ 500 ²³	150/ 500 ²³	150/ 500 ²³	150/ 500 ²³	500	500
Circuit-Teilnehmer ²¹ Die maximale Anzahl der Benutzer pro Netz hängt vom Typ des Hauptknotens ab.	150	30	150	150	150	150	150	150
Skype for Business-Teilnehmer	150/ 500 ²³	30	150/ 500 ²³	150/ 500 ²³	150/ 500 ²³	150/ 500 ²³	500	500

Tabelle 40: Ausbaustufe Teilnehmer/Benutzer mit OpenScape Business S

Teilnehmer	Basic Server (S)	Standard Server (S)	Advanced Server (S)
Teilnehmermaximum			
Max. Anzahl Teilnehmer	50	500	1500
IP-Teilnehmer			
IP-Teilnehmersystem (HFA)	50	500	1500
IP-Teilnehmer (SIP)	50	500	500
Mobility-Teilnehmer			
Max. Anzahl der Mobility-Teilnehmer	50	250	500
Mobility Entry-Teilnehmer	50	150	150
myPortal to go-Teilnehmer	50	250	500
myPortal for Teams-Teilnehmer	50	250	500
Circuit-Teilnehmer ²¹	50	150	250
Skype for Business-Teilnehmer	50	250	500

26.2 Maximalwerte für Leitungen

- Kanäle für alle Arten von Leitungen (Amts-, Quer-, Verbindungsleitungen usw.) in V2 OCC Mainboards finden Sie in [Tabelle 41: Ausbaustufe Leitungskanäle mit OCCx Mainboards](#) auf Seite 835.
- Kanäle für alle Arten von Leitungen (Amts-, Quer-, Verbindungsleitungen usw.) in V3 OCC Mainboards finden Sie in [Tabelle 42: Ausbaustufe Leitungskanäle mit OCCSB/R, OCCMA/B oder OCCLA Mainboards](#) auf Seite 836
- Kanäle für alle Arten von Leitungen (Amts-, Quer-, Verbindungsleitungen usw.) in OpenScape Business S finden Sie in [Tabelle 43: Ausbaustufe Leitungskanäle mit OpenScape Business S](#) auf Seite 837

Tabelle 41: Ausbaustufe Leitungskanäle mit OCCx Mainboards

	X1	X3W/R	X5W/R	X8
Maximale Leitungskanäle				
Max. Anzahl von Leitungskanälen ²⁴	250	250	250	250
Leitungskanäle für die Verbindung von Telefoniedienstanbieter, Vernetzung, externem Computer				
SIP-Leitungskanäle (ITSP)	30	60 ²⁵	60 ²⁵	60 ²⁵

²³ Werte sind gestaffelt nach Board-Version: Basic/Advanced

Ausbaugrenzen und Kapazitäten

	X1	X3W/R	X5W/R	X8
SIPQ-Kanäle (Vernetzung)	100	100	100	100
ISDN S ₀ - Kanäle (BRI)	4	20	52	128
ISDN S _{2M} - Kanäle (PRI)	-	30	30	80
ISDN CAS - Kanäle (PRI)	-	30	30	180
Analoge (a/b) Kanäle	-	X3R: 8 X3W: 16	X5R: 24 X5W: 48	120
Leitungskanäle für interne Zwecke				
MEB-Kanäle für interne Ansagen ²⁶	0	16	16	16
MEB-Leitungskanäle für UC Suite ²⁷	0	60 / 30 / 0 ²⁸	60 / 30 / 0 ²⁸	60 / 30 / 0 ²⁸

Tabelle 42: Ausbaustufe Leitungskanäle mit OCCSB/R, OCCMA/B oder OCCLA Mainboards

	X1W		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Maximale Leitungskanäle								
Max. Anzahl von Leitungskanälen ²⁴	250	250	250	250	250	250	250	250
Leitungskanäle für die Verbindung von Telefoniedienstleister, Vernetzung, externem Computer								
SIP-Leitungskanäle (ITSP)	60/ 120 ²⁹	120	120					
SIPQ-Kanäle (Vernetzung)	100	100	100	100	100	100	100	100
ISDN S ₀ - Kanäle (BRI)	-	-	16	16	48	48	128	128

²⁴ Summe von: SIP-Leitung, ITSP, SIPQ, TDM-Leitungskanäle und MEB-Leitungskanäle ohne (MEB-Ansagekanäle).

²⁵ Bei Vernetzung mit OpenScape Business S als ITSP-Gateway sind auch mehr als 60 Kanäle möglich

²⁶ Die MEB-Kanäle werden vom System für systeminterne Ansagen dynamisch belegt. Sie sind immer in der maximalen Anzahl von Leitungskanälen enthalten.

²⁷ Für Systeme mit UC Suite werden die MEB-Kanäle dynamisch generiert für: Voicemail, AutoAttendant, Fax, Call-Me-Verbindungen, Ansagen und Konferenzrufe. Sie gelten nur als Teil der maximalen Anzahl von Leitungskanälen in UC Suite-Systemen.

²⁸ Die Werte sind gestaffelt nach UC Booster-Konfiguration: Booster Server / Booster Card / ohne UC Booster

	X1W		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
ISDN S _{2M} - Kanäle (PRI)	-	-	30	30	30	30	180	120
ISDN CAS - Kanäle (PRI)	-	-	30	30	30	30	180	120
Analoge (a/b) Kanäle	-	-	X3R: 8 X3W: 16	X3R: 8 X3W: 16	X5R: 24 X5W: 48	X5R: 24 X5W: 48	120	120
Leitungskanäle für interne Zwecke								
MEB-Kanäle für interne Ansagen ²⁶	16	46	16	16	16	16	16	16
MEB-Leitungskanäle für UC Suite ²⁷	0	30/60 ²⁹	0	30/60 ²⁹	0	30/60 ²⁹	0	60

Tabelle 43: Ausbaustufe Leitungskanäle mit OpenScape Business S

	Basic Server (S)	Standard Server (S)	Advanced Server (S)
Maximale Leitungskanäle			
Max. Anzahl von Leitungskanälen ²⁴	250	250	250
Leitungskanäle für die Verbindung von Telefoniedienstanbieter, Vernetzung, externem Computer			
SIP-Leitungskanäle (ITSP)	180	180	180
SIPQ-Kanäle (Vernetzung)	100	100	100
Leitungskanäle für interne Zwecke			
MEB-Kanäle für interne Ansagen ²⁶	16	16	16
MEB-Leitungskanäle für UC Suite ²⁷	60	60	60

²⁹ Werte sind gestaffelt nach Board-Version: Basic/Advanced

Ausbaugrenzen und Kapazitäten

Maximalwerte der Ressourcen

26.3 Maximalwerte der Ressourcen

Tabelle 44: Ausbaustufen weitere Funktionen/Ressourcen

	X1		X3		X5		X8	Server (S)
	Wand	Rack	Wand	Rack	Wand	Rack	OCCL / OCCLA	
Systemressourcen								
DSP-Kanäle								
DSP G.711 ohne Verschlüsselung	8	128/ 48/ 8 ³⁵	n/a					
DSP G.711 + G.729 ohne Verschlüsselung	8	104/ 40/ 8 ³⁵	n/a					
DSP G.711 mit Verschlüsselung	6	102/ 38/ 6 ³⁵	n/a					
DSP G.711 + G.729 mit Verschlüsselung	6	81/ 31/ 6 ³⁵	n/a					
DSP Fax T.38 (für ISDN-Gateway) ³³	3	12/ 6/ 3 ³⁵	n/a					
DSP Fax T.38 (für UC Suite Fax) ³⁴	-	8/ 6/ 0 ³⁵	n/a					
RTP-Proxykanäle								
RTP-Proxykanäle	30	60	60	60	60	60	60	180
MEB-Leitungskanäle								
MEB-Leitungskanäle gesamt	0	76/ 46/ 0³¹	76					
MEB-Leitungskanäle für Ansagen	0	16/ 16/ 0 ³¹	16					
MEB-Leitungskanäle für UC Suite	-	60/ 30/ 0 ³¹	60					

	X1		X3		X5		X8	Server (S)
	Wand	Rack	Wand	Rack	Wand		OCCL / OCCLA	
Warteschleifenmusik und PPP								
MOH-Quellen ³⁰ (G.711a, G.711u, G.729ab, G.729a)	4	4	4	4	4	4	4	32
PPP-Kanäle	8	8	8	8	8	8	8	n/a
Ansagen								
Anzahl der Ansagegeräte pro System	16	16	16	16	16	16	16	16
Ansagegeräte über a/b	16	16	16	16	16	16	16	n/a
Ansagen über Smart VM	6	6	6	6	6	6	6	6
Ansage über UC-Suite	16	16	16	16	16	16	16	16
Ansage vor Beantwortung (System, nicht UC-Suite)								
Anzahl der Anrufer, für die eine Ansage gleichzeitig wiedergegeben werden kann	24	24	24	24	24	24	24	24
DTMF-Empfänger								
DTMF-Empfänger	16	16	16	16	16	16	16	Pro Gespräch via ITSP

³⁰ Max. Anzahl von 16 gleichzeitigen Verbindungen pro MOH-Quelle

³¹ Werte sind gestaffelt nach UC Booster-Konfiguration: Booster Server / Booster Card / ohne UC Booster

³² Der Wert ist abhängig von UC Suite: System mit UC Suite / System ohne UC Suite

³³ Werte gelten für OpenScape Business als ISDN-Gateway. G.711 zu T38 oder umgekehrt ohne UC Suite Fax

³⁴ UC Suite kann generell bis zu 8 gleichzeitige Faxverbindungen verarbeiten. OpenScape Business X3/X5/X8 als ISDN-Gateway kann abhängig vom DSP-Modul 3 bis 12 Faxe gleichzeitig verarbeiten. Beide Parameter in Kombination bestimmen die Anzahl der gleichzeitigen T.38- oder G.711-Faxverbindungen.

³⁵ Die Werte sind gestaffelt nach Voice Channel Booster-Konfiguration: mit OCCBH oder OCCB3 / mit OCCBL oder OCCB1 / nur Mainboard

26.3.1 Details zur Verwendung von DSP-Kanälen

Innerhalb von OpenScape Business werden „DSP-Kanäle“ für die Konvertierung (Transcodierung) von Datenströmen verwendet. Das ist grundsätzlich erforderlich, wenn es einen Übergang von IP zu TDM oder von TDM zu IP für die Sprachdaten gibt oder wenn eine Verschlüsselung der Sprachdaten erforderlich ist. Im Detail:

- Sprachverbindung zwischen IP-Telefon und ISDN- oder Analogleitung.
- Sprachverbindung über IP SIP/ITSP-Leitung und internen UPO/E-, a/b- oder ISDN-Telefonen.
- Sprachverbindung von IP-Leitung oder IP-Teilnehmer zu einer internen Konferenz. Hier ist ein Gatewaykanal für alle an einer Konferenz beteiligten Leitungen/IP-Clients erforderlich.
- Verbindungen von UPO/E-, a/b- oder ISDN-Telefonen oder ISDN-/Analogleitungen zu Ansagen, Voicemail, Fax oder Konferenzen in UC Suite.
- Verschlüsselte Sprachverbindungen zwischen Terminals und verschlüsselte Sprachverbindungen über ITSP-Leitungen.
- Verbindungen zu interner Warteschleifenmusik erfordern einen DSP-Kanal pro konfiguriertem MoH-Codec.

Für die folgenden Verbindungen ist kein DSP-Kanal erforderlich:

- Verbindung zwischen internen IP-Benutzern ohne Verschlüsselung (direkte Nutzlast)
- Verbindung zwischen ITSP und IP-Teilnehmer ohne Verschlüsselung. (direkte Nutzlast)

Die DSP-Kanäle werden durch einen Signalprozessor realisiert, der auf dem jeweiligen OCCL- oder OCCLA-Mainboard in den Modellen X1, X3, X5 und X8 integriert ist.

Je nach Art der Transcodierung kann ein Signalprozessor mehr oder weniger DSP-Kanäle gleichzeitig verarbeiten. Folgende Codierungen (Codecs) werden unterstützt:

- **Für Sprachverbindungen**
 - Konvertierung von IP (G.711) zu TDM mit G.711 oder umgekehrt.
 - Konvertierung von IP (G.711) zu TDM mit G.711 oder umgekehrt mit Verschlüsselung (SPE).
 - Konvertierung von IP (G.729) zu TDM mit G.711 oder umgekehrt.
 - Konvertierung von IP (G.729) zu TDM mit G.711 oder umgekehrt mit Verschlüsselung (SPE).
- **Für Faxverbindungen**
 - Konvertierung von T.38 zu G.711 bei Verwendung von OpenScape Business als ISDN-Gateway.
 - Konvertierung von G.711 Fax zu T.38 Fax oder umgekehrt bei Verwendung der Faxfunktion von UC Suite.

Wenn die Kapazität des auf dem Mainboard integrierten Signalprozessors nicht ausreicht, um die erforderliche Anzahl von DSP-Kanälen zu realisieren, können Sie mithilfe der optional

erhältlichen „Voice Channel Booster“-Karten OCCBL oder OCCBH erweitert werden.

Die maximale Anzahl der je nach Codierung verfügbaren DSP-Kanäle ist in Tabelle 11 angegeben. Bitte beachten Sie, dass jede Zeile die maximale Anzahl von ähnlichen DSP-Kanälen darstellt, aber diese im Betrieb vom System dynamisch zugewiesen werden. Die Anzahl der im Betrieb aktuell besetzten DSP-Kanäle kann über den OpenScape Business Assistant (WBM) bestimmt werden. Weitere Hinweise zur Bestimmung der erforderlichen Anzahl von DSP-Kanälen finden Sie im Administrationshandbuch.

26.3.2 Details zur Verwendung von RTP-Proxykanälen

OpenScape Business verwendet einen internen „RTP-Proxy“ für alle VoIP-Verbindungen über das Internet. Der Proxy bietet einen Pool von RTP-Kanälen, die den VoIP-Verbindungen über das Internet wie folgt zugeordnet sind:

- 1 RTP-Proxykanal pro ITSP-Anruf
- 1 RTP-Proxykanal pro Circuit-Anruf
- 1 RTP-Proxykanal pro Unify Phone-Anruf
- 1 RTP-Proxykanal pro System Device @Home in einem Anruf
- 1 RTP-Proxykanal pro SIP Device @Home in einem Anruf
- 1 RTP-Proxykanal pro myPortal to go VoIP @Home in einem Anruf
- 1 RTP-Proxykanal pro myPortal @work VoIP @Home in einem Anruf

In den verschiedenen OpenScape Business-Modellen ist eine verschiedene Anzahl von RTP-Proxykanälen verfügbar. Siehe [Tabelle 44: Ausbaustufen weitere Funktionen/Ressourcen](#) auf Seite 838.

Beispiele

- Ein externer abgehender Sprachanruf von einem internen IP-Systemteilnehmer über eine ISTP-Leitung erfordert einen RTP-Proxykanal.
- Ein externer Sprachanruf vom myPortal to go VoIP Client über internes WLAN (Campus) zu einem Teilnehmer im öffentlichen Netz über eine ITSP-Leitung erfordert einen RTP-Proxykanal. Dieser wird für die Verbindung über ITSP zum angerufenen Teilnehmer im öffentlichen Netz verwendet.
- Ein externer Sprachanruf vom myPortal to go VoIP-Client über öffentliches WLAN zu einem Teilnehmer im öffentlichen Netz über eine ITSP-Leitung erfordert zwei RTP-Proxykanäle. Ein RTP-Proxykanal ist für die Verbindung des VoIP-Clients zu OpenScape Business und ein anderer RTP-Proxykanal für die Verbindung über ITSP zum angerufenen Teilnehmer im öffentlichen Netz erforderlich.
- Ein externer Anruf, der über ITSP bei einem myPortal @work VoIP-Client im Homeoffice ankommt, erfordert zwei RTP-Proxykanäle. Ein RTP-Proxykanal ist für die Verbindung von ITSP zum OpenScape Business System und ein anderer für die Verbindung von OpenScape Business über das Internet zum myPortal @work VoIP-Client im Homeoffice erforderlich.

26.4 Maximalwerte für Leistungsmerkmale

Bei den hier beschriebenen Maximalwerten handelt es sich hauptsächlich um die Software-Kapazitäten von OpenScape Business.

26.4.1 Anbindung an Service-Provider

	X1/X1W		X3W/R		X5W/R		X8W/R		Server (S)
	V2	V3	V2	V3	V2	V3	V2	V3	
ITSP (Internet-Telefonie-Service-Provider)-Anbindung									
SIP-Leitungskanäle	30	120	60	120	60	120	60	120	180
Gleichzeitig aktivierter ITSP	8	8	8	8	8	8	8	8	8
Richtungen									
Richtungen	16	16	16	16	16	16	16	16	16
Überlaufschutz pro Richtung	1	1	1	1	1	1	1	1	1

26.4.2 Teilnehmer

	X1W	X3W/R	X5W/R	X8	Server (S)
Teilnehmerrufnummer/Durchwahlnummer					
Ziffern pro Teilnehmerrufnummer/Durchwahlnummer	16 (Standard = 3)				

26.4.3 UC Smart-Ausbaustufen

- Ausbaustufen mit V2 OCC Mainboards finden Sie in [Tabelle 45: Ausbaustufe UC SMART mit OCCx Mainboards](#) auf Seite 842
- Ausbaustufen mit V3 OCC Mainboards finden Sie in [Tabelle 46: Ausbaustufe UC Smart mit OCCSB/R, OCCMA/B oder OCCLA Mainboards](#) auf Seite 844
- Ausbaustufen mit OpenScape Business S Server-Systemen finden Sie in [Tabelle 47: Ausbaustufe UC Smart mit OpenScape Business S](#) auf Seite 845

Tabelle 45: Ausbaustufe UC SMART mit OCCx Mainboards

	X1	X3W/R	X5W/R	X8
UC Smart Benutzer maximal				

Ausbaugrenzen und Kapazitäten

	X1	X3W/R	X5W/R	X8
Max. Anzahl von UC Smart-Benutzern (Konten)	30	250/ 150/ 50 ³⁶	250/ 150/ 50 ³⁶	250/ 150/ 50 ³⁶
UC Smart Clients				
Anzahl der gleichzeitig aktiven UC-Clients. ³⁷	30	500/ 300/ 150 ³⁶	500/ 300/ 150 ³⁶	500/ 300/ 150 ³⁶
myPortal @work	30	250/ 150/ 50 ³⁶	250/ 150/ 50 ³⁶	250/ 150/ 50 ³⁶
myPortal @work Parallele Anrufe von VoIP zu anderen angerufenen Teilnehmern ³⁸	20	30	30	30
myPortal to go ³⁸	30	150/ 150/ 50 ³⁶	150/ 150/ 50 ³⁶	150/ 150/ 50 ³⁶
Deskphone CP 400/600/600E/ 700/700X/710 (UC-Modus)	30	250/ 150/ 50 ³⁶	250/ 150/ 50 ³⁶	250/ 150/ 50 ³⁶
OpenScape Business Attendant	8	8	8	8
Anwesenheitsstatus				
Status pro Benutzer	9	9	9	9
Sprachbox-Ansagen pro Anwesenheitsstatus	1	1	1	1
Favoriten				
Favoriten pro Benutzer	100	100	100	100
Favoritengruppen pro Benutzer	10	10	10	10
Anrufjournal				
Anrufjournalinträge pro Benutzer	100	100	100	100
UC Smart Verwaltete Konferenz (über UC Client)				
Anzahl der verwalteten Konferenzen	5	5	5	5
Anzahl der Benutzer pro verwalteter Konferenz	16	16	16	16
Kanäle für verwaltete Konferenzen	30	30	30	30

³⁶ Werte sind gestaffelt nach UC Booster-Konfiguration: Booster Server / Booster Card / ohne UC Booster

³⁷ Summe von: myPortal @work, myPortal to go, CP 400/600/600E/700/700X/710 UC-Modus, Application Launcher, Business Attendant, TAPI 120 (WSI), Drittanbieter-WSI-Clients (Hintergrund: Mehrere Clients mit dem gleichen UC Smart-Konto können sich am System anmelden)

³⁸ Die Anzahl der gleichzeitigen VoIP-Verbindungen des Teilnehmers hängt ab von:

Ausbaugrenzen und Kapazitäten

Tabelle 46: Ausbaustufe UC Smart mit OCCSB/R, OCCMA/B oder OCCLA Mainboards

	X1W		X3W/R		X5		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
UC Smart Benutzer maximal								
Max. Anzahl von UC Smart-Benutzern (Konten)	150	150	150/500 ⁴⁰	150/500 ⁴⁰	150/500 ⁴⁰	150/500 ⁴⁰	500	500
UC Smart Clients								
Anzahl der gleichzeitig aktiven UC-Clients. ³⁷	150	150	150/500 ⁴⁰	300 / 1000	150/500 ⁴⁰	300/1000 ⁴⁰	1000	1000
myPortal @work	150	150	150/250 ⁴⁰	150/250 ⁴⁰	150/250 ⁴⁰	150/250 ⁴⁰	250	250
myPortal @work Parallele Anrufe von VoIP zu anderen angerufenen Teilnehmern ³⁸	150	150	30/ 70 ⁴⁰	30/ 70 ⁴⁰	30/ 70 ⁴⁰	30/ 70 ⁴⁰	70	70
myPortal to go ³⁸	150	150	150/500 ⁴⁰	150/500 ⁴⁰	150/500 ⁴⁰	150/500 ⁴⁰	500	500
myPortal for Teams	150	150	150/500 ⁴⁰	150/500 ⁴⁰	150/500 ⁴⁰	150/500 ⁴⁰	500	500
Deskphone CP 400/600/600E/ 700/700X/710 (UC-Modus)	150	150	150/500 ⁴⁰	150/500 ⁴⁰	150/500 ⁴⁰	150/500 ⁴⁰	500	500
OpenScope Business Attendant	8	8	8	8	8	8	8	8
Anwesenheitsstatus								
Status pro Benutzer	9	9	9	9	9	9	9	9

1) den im System verfügbaren DSP-Kanälen für Gateway-Anrufe (IP/TDM-Übergang).

2) den im System verfügbaren internen RTP-Proxykanälen für VoIP-Anrufe über das Internet.

³⁹ der Anzahl der gleichzeitigen Verbindung je nach den im System verfügbaren DSP-Kanälen für Gateway-Anrufe (IP/TDM-Übergang).

	X1W		X3W/R		X5		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Sprachbox-Ansagen pro Anwesenheitsstatus	1	1	1	1	1	1	1	1
Favoriten								
Favoriten pro Benutzer	100	100	100	100	100	100	100	100
Favoritengruppen pro Benutzer	10	10	10	10	10	10	10	10
Anrufjournal								
Anrufjournalinträge pro Benutzer	100	100	100	100	100	100	100	100
UC Smart Verwaltete Konferenz (über UC Client)								
Anzahl der verwalteten Konferenzen	5	5	5	5	5	5	5	5
Anzahl der Benutzer pro verwalteter Konferenz	16	16	16	16	16	16	16	16
Kanäle für verwaltete Konferenzen	30	30	30	30	30	30	30	30

Tabelle 47: Ausbaustufe UC Smart mit OpenScape Business S

	Basic Server (S)	Standard Server (S)	Advanced Server (S)
UC Smart Benutzer maximal			
Max. Anzahl von UC Smart-Benutzern (Konten)	50	500	1500
UC Smart Clients			
Anzahl der gleichzeitig aktiven UC-Clients. ³⁷	50	500	1500
myPortal @work	50	250	500
myPortal to go ³⁸	50	250	500
myPortal for Teams	50	250	500

⁴⁰ Werte sind gestaffelt nach Board-Version: Basic/Advanced

Ausbaugrenzen und Kapazitäten

	Basic Server (S)	Standard Server (S)	Advanced Server (S)
Deskphone CP 400/600/600E/ 700/700X/710 (UC-Modus)	50	250	500
OpenScape Business Attendant	8	8	8
Anwesenheitsstatus			
Status pro Benutzer	9	9	9
Sprachbox-Ansagen pro Anwesenheitsstatus	1	1	1
Favoriten			
Favoriten pro Benutzer	100	100	100
Favoritengruppen pro Benutzer	10	10	10
Anrufjournal			
Anrufjournalinträge pro Benutzer	100	100	100
UC Smart Verwaltete Konferenz (über UC Client)			
Anzahl der verwalteten Konferenzen	10	10	10
Anzahl der Benutzer pro verwalteter Konferenz	16	16	16
Kanäle für verwaltete Konferenzen	30	30	30

26.4.4 Smart Voicemail Ausbaustufen

- Ausbaustufen mit V2 OCC Mainboards finden Sie in [Tabelle 48: Ausbaustufe Smart Voicemail mit OCCx Mainboards](#) auf Seite 846
- Ausbaustufen mit V3 OCC Mainboards finden Sie in [Tabelle 49: Ausbaustufe Smart Voicemail mit OCCSB/R, OCCMA/B oder OCCLA Mainboards](#) auf Seite 847
- Ausbaustufen mit OpenScape Business S Server-Systemen finden Sie in [Tabelle 50: Ausbaustufe Smart Voicemail mit OpenScape Business S](#) auf Seite 847

Tabelle 48: Ausbaustufe Smart Voicemail mit OCCx Mainboards

	X1	X3W/R	X5W/R	X8	Server (S)
Smart Voicemail					
Smart Voicemail-Boxen	30	320	320	320	1500
Nachrichten pro Voicemail-Box	100	100	100	100	100
Aufzeichnungszeit pro Anruf (Minuten)	2	2	2	2	2

	X1	X3W/R	X5W/R	X8	Server (S)
Gesamtaufnahmekapazität in Stunden	32	32	32	32	32
Gleichzeitige Voicemail-Verbindungen (Kanäle)	10	10	10	10	60
Ansagen	16	16	16	16	16
Company/AutoAttendants	100	100	100	100	100
Company/AutoAttendants (gleichzeitig aktiv)	6	6	6	6	6

Tabelle 49: Ausbaustufe Smart Voicemail mit OCCSB/R, OCCMA/B oder OCCLA Mainboards

	X1W		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Smart Voicemail								
Smart Voicemail-Boxen	320	320	320/500 ⁴¹	320/500 ⁴¹	320/500 ⁴¹	320/500 ⁴¹	500	500
Nachrichten pro Voicemail-Box	100	100	100	100	100	100	100	100
Aufzeichnungszeit pro Anruf (Minuten)	2	4	4	4	4	4	4	4
Gesamtaufnahmekapazität in Stunden	32	64	32	64	32	64	32	64
Gleichzeitige Voicemail-Verbindungen (Kanäle)	30	30	30	30	30	30	30	30
Ansagen	16	16	16	16	16	16	16	16
Company/AutoAttendants	100	100	100	100	100	100	100	100
Company/AutoAttendants (gleichzeitig aktiv)	6	6	6	6	6	6	6	6

Tabelle 50: Ausbaustufe Smart Voicemail mit OpenScape Business S

	Basic Server (S)	Standard Server (S)	Advanced Server (S)
Smart Voicemail			

⁴¹ Werte sind gestaffelt nach Board-Version: Basic/Advanced

Ausbaugrenzen und Kapazitäten

	Basic Server (S)	Standard Server (S)	Advanced Server (S)
Smart Voicemail-Boxen	1500	1500	1500
Nachrichten pro Voicemail-Box	100	100	100
Aufzeichnungszeit pro Anruf (Minuten)	4	4	4
Gesamtaufnahmekapazität in Stunden	64	64	64
Gleichzeitige Voicemail-Verbindungen (Kanäle)	60	60	60
Ansagen	16	16	16
Company/AutoAttendants	100	100	100
Company/AutoAttendants (gleichzeitig aktiv)	6	6	6

26.4.5 UC Suite-Ausbaustufen

- Ausbaustufen mit V2 OCC Mainboards finden Sie in [Tabelle 51: Ausbaustufe UC Suite mit V2 Mainboards](#) auf Seite 848
- Ausbaustufen mit V3 OCC Mainboards finden Sie in [Tabelle 52: Ausbaustufe UC Suite mit OCCSB, OCCMA/B oder OCCLA Mainboards](#) auf Seite 851
- Ausbaustufen mit OpenScope Business S Server-Systemen finden Sie in [Tabelle 53: Ausbaustufe UC Suite mit OpenScope Business S](#) auf Seite 855

Tabelle 51: Ausbaustufe UC Suite mit V2 Mainboards

	X1	X3W/R	X5W/R	X8	Server (S)
UC Suite Benutzer maximal					
Max. Anzahl von UC Suite-Benutzern (Konten)	-	250/ 150/ 0 ⁴²	250/ 150/ 0 ⁴²	250/ 150/ 0 ⁴²	1500
UC Suite Clients					
Anzahl der gleichzeitig aktiven UC-Clients. ⁴³	-	500/ 150/ 0 ⁴²	500/ 150/ 0 ⁴²	500/ 150/ 0 ⁴²	1500
myPortal for Desktop	-	500/ 150/ 0 ⁴²	500/ 150/ 0 ⁴²	500/ 150/ 0 ⁴²	1500
myPortal for Outlook	-	500/ 150/ 0 ⁴²	500/ 150/ 0 ⁴²	500/ 150/ 0 ⁴²	1500
myAgent (gleichzeitig aktiv)	-	64	64	64	64
myAgent (konfigurierbar)	-	192	192	192	192

Ausbaugrenzen und Kapazitäten

	X1	X3W/R	X5W/R	X8	Server (S)
myReports	-	1	1	1	1
myAttendant	-	20	20	20	20
myPortal @work	-	250/ 150/ 0 ⁴²	250/ 150/ 0 ⁴²	250/ 150/ 0 ⁴²	250
myPortal @work Parallele Anrufe von VoIP zu anderen angerufenen Teilnehmern ⁴⁵	-	30	30	30	60
myPortal to go ⁴⁵	-	150/ 150/ 0 ⁴²	150/ 150/ 0 ⁴²	150/ 150/ 0 ⁴²	250
Deskphone 400/600/600E/700/700X/710	-	250/ 150/ 0 ⁴²	250/ 150/ 0 ⁴²	250/ 150/ 0 ⁴²	250
OpenScape Business Attendant	-	8	8	8	8
Anwesenheitsstatus					
Status pro UC Suite Teilnehmer	-	9	9	9	9
Sprachbox-Ansagen pro Anwesenheitsstatus	-	1	1	1	1
Anrufjournal (myPortal for Desktop/myPortal for Outlook)					
Archivierungsdauer in den UC Clients (Tage)	-	30 Standard = 30	30 Standard = 30	30 Standard = 30	30 Standard = 30
Archivierungsdauer im Kommunikationssystem	-	365 Standard = 30	365 Standard = 30	365 Standard = 30	365 Standard = 30
Anrufjournalinträge ⁴⁷	-	Uneingeschränkt ⁴⁷	Uneingeschränkt ⁴⁷	Uneingeschränkt ⁴⁷	Uneingeschränkt ⁴⁷
Anrufjournalinträge myPortal for Desktop modernes GUI	-	100 nach Inbetriebnahme >100 im Betrieb	100 nach Inbetriebnahme >100 im Betrieb	100 nach Inbetriebnahme >100 im Betrieb	100 nach Inbetriebnahme >100 im Betrieb
UC Suite Voicemail					
VM-Boxen	-	500/ 500/ 0 ⁴⁶	500/ 500/ 0 ⁴⁶	500/ 500/ 0 ⁴⁶	1500
VM-Gruppen	-	20/ 20/ 0	20/ 20/ 0	20/ 20/ 0	20
Nachrichten pro Sprachbox ⁴⁷	-	n/a	n/a	n/a	n/a
Aufzeichnungsdauer pro Anruf (Minuten)	-	15	15	15	15

Ausbaugrenzen und Kapazitäten

	X1	X3W/R	X5W/R	X8	Server (S)
Aufzeichnungsdauer zur Weiterleitung per E-Mail (Minuten) ⁴⁸	-	~10	~10	~10	~10
Gesamtaufnahmekapazität (Stunden) ⁴⁷	-	n/a	n/a	n/a	n/a
Gleichzeitige Verbindungen zu Voicemail (MEB-Kanäle)	-	30	30	30	60
UC Suite AutoAttendant					
Personal AutoAttendant	-	20/ 20/ 0 ⁴²	20/ 20/ 0 ⁴²	20/ 20/ 0 ⁴²	20
Company AutoAttendant	-	1/ 1/ 0 ⁴²	1/ 1/ 0 ⁴²	1/ 1/ 0 ⁴²	1
Multi-User-Chat (Instant Messaging)					
Interne Kommunikationspartner	-	unbeschränkt	unbeschränkt	unbeschränkt	unbeschränkt
Externe Kommunikationspartner (XMPP)	-	-	-	-	-
Ansagen pro UC Suite Benutzer					
Begrüßungsansagen	-	1/ 1/ 0 ⁴²	1/ 1/ 0 ⁴²	1/ 1/ 0 ⁴²	1
Ansagen basierend auf Anwesenheitsstatus	-	1/ 1/ 0 ⁴²	1/ 1/ 0 ⁴²	1/ 1/ 0 ⁴²	1
Ansage Personal AutoAttendant	-	1/ 1/ 0 ⁴²	1/ 1/ 0 ⁴²	1/ 1/ 0 ⁴²	1
UC Suite Anrufaufzeichnung					
Aufzeichnungsdauer pro Anruf/Konferenz	-	Begrenzt durch Anrufdauer	Begrenzt durch Anrufdauer	Begrenzt durch Anrufdauer	Begrenzt durch Anrufdauer
UC Suite Fax					
Faxboxen	-	500/ 150/ 0 ⁴²	500/ 150/ 0 ⁴²	500/ 150/ 0 ⁴²	1500
Faxbox-Gruppen	-	60/ 60/ 0 ⁴²	60/ 60/ 0 ⁴²	60/ 60/ 0 ⁴²	60
Teilnehmer pro Faxbox-Gruppe	-	10/ 10/ 0 ⁴²	10/ 10/ 0 ⁴²	10/ 10/ 0 ⁴²	10
Faxlänge in Seiten	-	500/ 500/ 0 ⁴²	500/ 500/ 0 ⁴²	500/ 500/ 0 ⁴²	500
Gleichzeitige T.38 Faxgeräte	-	8/ 3/ 0 ⁴²	8/ 3/ 0 ⁴²	8/ 3/ 0 ⁴²	8
Serienfaxempfänger	-	unbeschränkt	unbeschränkt	unbeschränkt	unbeschränkt
UC Suite Konferenzen					

	X1	X3W/R	X5W/R	X8	Server (S)
Gleichzeitige UC Suite Konferenzen	-	5/ 5/ 0 ⁴²	5/ 5/ 0 ⁴²	5/ 5/ 0 ⁴²	10
Teilnehmer pro UC Suite Konferenz	-	16/ 16/ 0 ⁴²	16/ 16/ 0 ⁴²	16/ 16/ 0 ⁴²	16
Externe Teilnehmer als Benutzer pro UC Suite Konferenz	-	15/ 15/ 0 ⁴²	15/ 15/ 0 ⁴²	15/ 15/ 0 ⁴²	15
Max. Anzahl Kanäle für UC Suite Konferenzen	-	30/ 30/ 0 ⁴²	30/ 30/ 0 ⁴²	30/ 30/ 0 ⁴²	60
Anzahl der reservierten Kanäle für UC Suite Ad-hoc- und Meet-Me-Konferenzen	-	20/ 20/ 0 ⁴²	20/ 20/ 0 ⁴²	20/ 20/ 0 ⁴²	60
Externe Datenbankbindung (LDAP)					
Externe Datenbankverbindungen von UC Server	-	10/ 10/ 0 ⁴²	10/ 10/ 0 ⁴²	10/ 10/ 0 ⁴²	10

Tabelle 52: Ausbaustufe UC Suite mit OCCSB, OCCMA/B oder OCCLA Mainboards

	X3W/R		X5W/R		X8
		+ NVMe SSD		+ NVMe SSD	+ NVMe SSD
UC Suite Benutzer maximal					

⁴² Werte sind gestaffelt nach UC Booster-Konfiguration: Booster Server / Booster Card / ohne UC Booster

⁴³ Summe von: myPortal Desktop, myPortal for Outlook, myAttendant, myAgent, myReports, myPortal @work, myPortal to go, myPortal for Teams, CP 400/600/600E/700/700X/710 UC-Modus (Hintergrund: Mehrere Clients mit dem gleichen UC Suite-Konto können sich am System anmelden)

⁴⁴ Der niedrigere Wert gilt für Systeme mit UC Suite Contact Center

⁴⁵ Die Anzahl der gleichzeitigen VoIP-Verbindungen des Teilnehmers hängt ab von

1) den im System verfügbaren DSP-Kanälen für Gateway-Anrufe (IP/TDM-Übergang).

2) den im System verfügbaren internen RTP-Proxykanälen für VoIP-Anrufe über das Internet.

⁴⁶ Die UC Booster Card unterstützt maximal 500 Voicemail-Boxen, unabhängig vom UC Suite Client-Limit (150 Benutzer).

⁴⁷ Der Wert hängt von der verfügbaren HD-/SSD-Speicherkapazität der Festplatte ab. Eine teilnehmerbezogene Begrenzung ist nicht implementiert.

1) Voicemail / Aufzeichnungen: Eine Minute Aufnahmezeit benötigt ca. 1 MB Speicherplatz

2) Fax: Ein Normfax (2 DIN-A4-Seiten) entspricht ca. 48 KB Speicherbedarf

Beispiel: Das Speichervolumen der Partition für die Aufzeichnung von Sprachansagen, Sprachnachrichten, Sprachanrufe und Faxe beträgt 20 GB auf einer Festplatte mit 160 GB. Das entspricht einer Gesamtaufzeichnungsdauer von ca. 20.000 Minuten.

⁴⁸ Bei längeren Aufzeichnungen wird die Aufnahme in mehrere Dateien aufgeteilt und gesendet.

Ausbaugrenzen und Kapazitäten

	X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Max. Anzahl von UC Suite-Benutzern (Konten)	-	50/ 500 ⁴⁹ 300 bei Contact Center	-	50/ 500 ⁴⁹	-	500 300 bei Contact Center
UC Suite Clients						
Anzahl der gleichzeitig aktiven UC-Clients. ⁴³	-	100/ 1000 ⁴⁹ 600 bei Contact Center	-	100/ 1000 ⁴⁹ 600 bei Contact Center	-	1000 600 bei Contact Center
myPortal for Desktop	-	50/ 500 ⁴⁹ 300 bei Contact Center	-	50/ 500 ⁴⁹ 300 bei Contact Center	-	500 300 bei Contact Center
myPortal for Outlook	-	50/ 500 ⁴⁹ 300 bei Contact Center	-	50/ 500 ⁴⁹ 300 bei Contact Center	-	500 300 bei Contact Center
myAgent (gleichzeitig aktiv)	-	0/ 64 ⁴⁹	-	0/ 64 ⁴⁹	-	64
myAgent (konfigurierbar)	-	0/ 192 ⁴⁹	-	0/ 192 ⁴⁹	-	192
myReports	-	0/ 1 ⁴⁹	-	0/ 1 ⁴⁹	-	1
myAttendant	-	4/ 20 ⁴⁹	-	4/ 20 ⁴⁹	-	20
myPortal @work	-	50/ 250 ⁴⁹ 300 bei Contact Center	-	50/ 250 ⁴⁹ 300 bei Contact Center	-	250 300 bei Contact Center
myPortal @work Parallele Anrufe von VoIP zu anderen angerufenen Teilnehmern ⁴⁵	-	30/ 70 ⁴⁹	-	30/ 70 ⁴⁹	-	70
myPortal to go ⁴⁵	-	50/ 500 ⁴⁹ 300 bei Contact Center	-	50/ 500 ⁴⁹ 300 bei Contact Center	-	500 300 bei Contact Center

Ausbaugrenzen und Kapazitäten

	X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
myPortal for Teams	-	50/ 500 ⁴⁹ 300 bei Contact Center	-	50/ 500 ⁴⁹ 300 bei Contact Center	-	500 300 bei Contact Center
Deskphone CP 400/600/600E/ 700/700X/710	-	50/ 500 ⁴⁹ 300 bei Contact Center	-	50/ 500 ⁴⁹ 300 bei Contact Center	-	500 300 bei Contact Center
OpenScape Business Attendant	-	8	-	8	-	8
Anwesenheitsstatus						
Status pro UC Suite Teilnehmer	-	9	-	9	-	9
Sprachbox-Ansagen pro Anwesenheitsstatus	-	1	-	1	-	1
Anrufjournal (myPortal for Desktop/myPortal for Outlook)						
Archivierungsdauer in den UC Clients (Tage)	-	30 Standard = 30	-	30 Standard = 30	-	30 Standard = 30
Archivierungsdauer im Kommunikationssystem	-	365 Standard = 30	-	365 Standard = 30	-	365 Standard = 30
Anrufjournalinträge ⁴⁷	-	Uneingeschränkt ⁴⁷	-	Uneingeschränkt ⁴⁷	-	Uneingeschränkt ⁴⁷
Anrufjournalinträge myPortal for Desktop modernes GUI	-	100 nach Inbetriebnahme >100 im Betrieb	-	100 nach Inbetriebnahme >100 im Betrieb	-	100 nach Inbetriebnahme >100 im Betrieb
UC Suite Voicemail						
VM-Boxen	-	50/ 500 ⁴⁹	-	50/ 500 ⁴⁹	-	500
VM-Gruppen	-	32	-	32	-	32
Nachrichten pro Sprachbox ⁴⁷	-	n/a	-	n/a	-	n/a
Aufzeichnungsdauer pro Anruf (Minuten)	-	15	-	15	-	15
Aufzeichnungsdauer zur Weiterleitung per E-Mail (Minuten) ⁴⁸	-	~10	-	~10	-	~10

Ausbaugrenzen und Kapazitäten

	X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Gesamtaufnahmekapazität (Stunden) ⁴⁷		n/a	-	n/a	-	n/a
Gleichzeitige Verbindungen zu Voicemail (MEB-Kanäle)	-	30/ 60 ⁴⁹	-	30/ 60 ⁴⁹	-	60
UC Suite AutoAttendant						
Personal AutoAttendant	-	20	-	20	-	20
Company AutoAttendant	-	1	-	1	-	1
Multi-User-Chat (Instant Messaging)						
Interne Kommunikationspartner	-	unbeschränkt	-	unbeschränkt	-	unbeschränkt
Ansagen pro UC Suite Benutzer						
Begrüßungsansagen	-	1	-	1	-	1
Ansagen basierend auf Anwesenheitsstatus	-	1	-	1	-	1
Ansage Personal AutoAttendant	-	1	-	1	-	1
UC Suite Anrufaufzeichnung						
Aufzeichnungsdauer pro Anruf/Konferenz	-	Begrenzt durch Anrufdauer	-	Begrenzt durch Anrufdauer	-	Begrenzt durch Anrufdauer
UC Suite Fax						
Faxboxen	-	50/ 500 ⁴⁹	-	50/ 500 ⁴⁹	-	500
Faxbox-Gruppen	-	60	-	60	-	60
Teilnehmer pro Faxbox-Gruppe	-	10	-	10	-	10
Faxlänge in Seiten	-	500	-	500	-	500
Gleichzeitige T.38 Faxgeräte	-	3/ 8 ⁴⁹	-	3/ 8 ⁴⁹	-	8
Serienfaxempfänger	-	unbeschränkt	-	unbeschränkt	-	unbeschränkt
UC Suite Konferenzen						
Gleichzeitige UC Suite Konferenzen	-	5	-	5	-	5
Teilnehmer pro UC Suite Konferenz	-	16	-	16	-	16

	X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Externe Teilnehmer als Benutzer pro UC Suite Konferenz	-	15	-	15	-	15
Max. Anzahl Kanäle für UC Suite Konferenzen	-	30	-	30	-	30
Anzahl der reservierten Kanäle für UC Suite Ad-hoc- und Meet-Me-Konferenzen	-	20	-	20	-	20
Externe Datenbankanbindung (LDAP)						
Externe Datenbankverbindungen von UC Server	-	10	-	10	-	10

Tabelle 53: Ausbaustufe UC Suite mit OpenScape Business S

	Basic Server (S)	Standard Server (S)	Advanced Server (S)
UC Suite Benutzer maximal			
Max. Anzahl von UC Suite-Benutzern (Konten)	150	500	1500
UC Suite Clients			
Anzahl der gleichzeitig aktiven UC-Clients. ⁴³	150	500	1500
myPortal for Desktop	50	500	1500
myPortal for Outlook	50	500	1500
myAgent (gleichzeitig aktiv)	0	64	64
myAgent (konfigurierbar)	0	192	192
myReports	1	1	1
myAttendant	20	20	20
myPortal @work	50	250	500
myPortal @work	30	60	60
Parallele Anrufe von VoIP zu anderen angerufenen Teilnehmern ⁴⁵			

⁴⁹ Werte sind gestaffelt nach Board-Version: Basic/Advanced

Ausbaugrenzen und Kapazitäten

	Basic Server (S)	Standard Server (S)	Advanced Server (S)
myPortal to go ⁴⁵	50	250	500
myPortal for Teams	50	250	500
Deskphone CP 400/600/600E/ 700/700X/710	50	250	500
OpenScape Business Attendant	8	8	8
Anwesenheitsstatus			
Status pro UC Suite Teilnehmer	9	9	9
Sprachbox-Ansagen pro Anwesenheitsstatus	1	1	1
Anrufjournal (myPortal for Desktop/myPortal for Outlook)			
Archivierungsdauer in den UC Clients (Tage)	30 Standard = 30	30 Standard = 30	30 Standard = 30
Archivierungsdauer im Kommunikationssystem	365 Standard = 30	365 Standard = 30	365 Standard = 30
Anrufjournalinträge ⁴⁷	Uneingeschränkt ⁴⁷	Uneingeschränkt ⁴⁷	Uneingeschränkt ⁴⁷
Anrufjournalinträge myPortal for Desktop modernes GUI	100 nach Inbetriebnahme >100 im Betrieb	100 nach Inbetriebnahme >100 im Betrieb	100 nach Inbetriebnahme >100 im Betrieb
UC Suite Voicemail			
VM-Boxen	150	500	1500
VM-Gruppen	32	32	32
Nachrichten pro Sprachbox ⁴⁷	n/a	n/a	n/a
Aufzeichnungsdauer pro Anruf (Minuten)	15	15	15
Aufzeichnungsdauer zur Weiterleitung per E-Mail (Minuten) ⁴⁸	~10	~10	~10
Gesamtaufnahmekapazität (Stunden) ⁴⁷	n/a	n/a	n/a
Gleichzeitige Verbindungen zu Voicemail (MEB-Kanäle)	60	60	60
UC Suite AutoAttendant			
Personal AutoAttendant	20	20	20
Company AutoAttendant	1	1	1
Multi-User-Chat (Instant Messaging)			

	Basic Server (S)	Standard Server (S)	Advanced Server (S)
Interne Kommunikationspartner	unbeschränkt	unbeschränkt	unbeschränkt
Ansagen pro UC Suite Benutzer			
Begrüßungsansagen	1	1	1
Ansagen basierend auf Anwesenheitsstatus	1	1	1
Ansage Personal AutoAttendant	1	1	1
UC Suite Anrufaufzeichnung			
Aufzeichnungsdauer pro Anruf/ Konferenz	Begrenzt durch Anrufdauer	Begrenzt durch Anrufdauer	Begrenzt durch Anrufdauer
UC Suite Fax			
Faxboxen	1500	1500	1500
Faxbox-Gruppen	60	60	60
Teilnehmer pro Faxbox-Gruppe	10	10	10
Faxlänge in Seiten	500	500	500
Gleichzeitige T.38 Faxgeräte	8	8	8
Serienfaxempfänger	unbeschränkt	unbeschränkt	unbeschränkt
UC Suite Konferenzen			
Gleichzeitige UC Suite Konferenzen	10	10	10
Teilnehmer pro UC Suite Konferenz	16	16	16
Externe Teilnehmer als Benutzer pro UC Suite Konferenz	15	15	15
Max. Anzahl Kanäle für UC Suite Konferenzen	60	60	60
Anzahl der reservierten Kanäle für UC Suite Ad-hoc- und Meet-Me-Konferenzen	60	60	60
Externe Datenbankanbindung (LDAP)			
Externe Datenbankverbindungen von UC Server	10	10	10

26.4.6 Funktionen am Telefon

	X1W	X3W/R	X5W/R	X8W/R	Server (S)
Anruferliste für Systemtelefone (HFA)					
Anruferlisten pro System	650	650	650	650	1300
Anruferlisten pro Teilnehmer im System	1	1	1	1	1
Einträge pro Anruferliste	10	10	10	10	10

Ausbaugrenzen und Kapazitäten

	X1W	X3W/R	X5W/R	X8W/R	Server (S)
Gespeicherte Ziffern pro Eintrag plus Belegungskennzahl	25 + (6)				
Direktruftasten (DSS-Tasten)					
Beistellgeräte pro Kommunikationssystem	250	250	250	250	250
Beistellgeräte pro Telefon	2	2	2	2	2
Tasten pro OpenStage Beistellgerät	12	12	12	12	12
Tasten pro OpenStage Beistellgerät 15	18	18	18	18	18
Besetztlampenfelder (BLF) pro Kommunikationssystem	12	25	25	25	25
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 (plus Belegungskennzahl)	25 (+ 6)				
Kurzwahl zentral (KWZ)					
Einträge im KWI-Pool pro Kommunikationssystem	8000	8000	8000	8000	8000
Zeichenlänge des Namens	16	16	16	16	16
Ziffern pro Eintrag (plus Belegungskennzahl)	25 (+ 6)				
Wahlwiederholung					
Einträge pro OpenStage 20/ 20E/ 20G/ 40/ 40G	3	3	3	3	3
Einträge pro OpenStage 15	10	10	10	10	10
Einträge pro OpenStage 60/ 60G/ 80/ 80G	30	30	30	30	30
Einträge pro Telefon ohne Display	1	1	1	1	1
Gespeicherte Ziffern pro Eintrag	25 (+ 6)				
Anklopfen/Rufeinblendung					

	X1W	X3W/R	X5W/R	X8W/R	Server (S)
Wartende Anrufer pro Telefon	16				
Parken					
Parkpositionen pro System	10				
Rückrufe					
Rückrufeinträge pro Telefon	5				
Abwesenheitstexte/Mitteilungstexte					
Abwesenheitstexte pro System	250	250	250	250	250
Mitteilungstexte pro System	150	150	150	150	150
Konfigurierbare Abwesenheitstexte + Mitteilungstexte pro System	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				
Anrufumleitung (AUL)					
AUL-Ziele pro Telefon	4	4	4	4	4
Zeichen pro externem AUL-Ziel (plus Belegungskennzahl)	25 (+ 6)	25 (+ 6)	25 (+ 6)	25 (+ 6)	25 (+ 6)
Verkettete AUL-Ziele					5
Systemgesteuerte Konferenzen					
Gleichzeitige System-Konferenzen pro System	10	10	10	10	8
Teilnehmer pro Konferenz	8	8	8	8	8
Externe Teilnehmer pro Konferenz	7	7	7	7	7
Konferenzkanäle	32	32	32	32	20

Ausbaugrenzen und Kapazitäten

	X1W	X3W/R	X5W/R	X8W/R	Server (S)
Türsprechstelle/Türöffner					
Anschlüsse über a/b-Schnittstellen pro System	4	4	4	4	-
Ziffern pro Codeeintrag	5	5	5	5	-
Leitungsvormerken					
Gleichzeitige Einträge pro System	32	32	32	32	-

Anmerkung: Für alle oben genannten Szenarien der Anrufumleitung kann der Benutzer nur ein Weberschaltungsziel pro MSN eingeben. Die maximale Anzahl weberschaltbarer MSN ist 10.

Falls ITSP oder ISDN mit der Durchwahl konfiguriert ist, lautet diese Nummer 249.

26.4.7 Arbeiten im Team (Gruppen)

- Informationen zu V2 OCC Mainboards finden Sie in [Tabelle 54: Daten für V2 Mainboards](#) auf Seite 860
- Informationen zu V3 OCC Mainboards finden Sie in [Tabelle 55: Daten für V3 Mainboards](#) auf Seite 862
- Informationen zu OpenScape Business S Server-Systemen finden Sie in [Tabelle 56: Daten für OpenScape Business S](#) auf Seite 864

Tabelle 54: Daten für V2 Mainboards

	X1	X3W/R	X5W/R	X8
Anrufübernahmegruppen				
Anrufübernahmegruppen pro System	32	32	32	32
Teilnehmer pro Anrufübernahmegruppe	32	32	32	32
Rufzuschaltung (benutzerkonfigurierbare Gruppe)				
Anzahl der Nebenstellen in der Rufzuschaltungsgruppe	5	5	5	5
Gruppenruf, Sammelanschluss, Basic-MULAPs				
Summe der Gruppenrufe, Sammelanschlüsse, Basic-MULAPs, Chef-MULAPs und Sprachbox-Gruppen pro Kommunikationssystem	800	800	800	800
Länge des Gruppennamens	16	16	16	16

	X1	X3W/R	X5W/R	X8
Anzahl der Gruppen, denen ein Benutzer zugewiesen werden kann	32	32	32	32
Teilnehmer pro Gruppenruf, Sammelanschluss, Basic-MULAP	20	20	20	20
Chef-MULAPs, Team-Gruppen, Top-Gruppen und Voicemail-Gruppen:				
Summe der Chef-MULAPs, Team- und Top-Gruppen pro	500	500	500	500
Teilnehmer pro Chef-MULAP, Team-Gruppe, Top-Gruppe	10	10	10	10
MULAP-Tasten pro Telefon	10	10	10	10
Voicemail-Gruppen				
Anzahl der Voicemail-Gruppen	20	20	20	20
Teilnehmer pro Sprachbox-Gruppe	20	20	20	20
Durchsage an Gruppe (Sprachdurchsage)				
Gleichzeitige Durchsagen pro Kommunikationssystem	1	1	1	1
Empfänger der Durchsage	20	20	20	20
UCD-Gruppen				
UCD-Gruppen pro System	60	60	60	60
Ansagen pro UCD-Gruppe	7	7	7	7
Prioritätsebenen pro UCD-Gruppe	10	10	10	10
Wartende Anrufe pro UCD-Gruppe (letzte Gruppe max. 72)	30	30	30	30
UCD-Agenten				
UCD-Agenten-IDs pro Kommunikationssystem	330	330	330	330
Gleichzeitig aktive UCD-Agenten pro Kommunikationssystem	64	64	64	64
UCD-Ansagen				
Anrufer pro Kommunikationssystem, denen gleichzeitig eine Ansage eingespielt werden kann	8	8	8	8

Ausbaugrenzen und Kapazitäten

Tabelle 55: Daten für V3 Mainboards

	X1W		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Anrufübernahmegruppen								
Anrufübernahmegruppen pro System	64	64	64/128 ⁵⁰	64/128 ⁵⁰	64/128 ⁵⁰	64/128 ⁵⁰	128	128
Teilnehmer pro Anrufübernahmegruppe	32	32	32	32	32	32	32	32
Rufzuschaltung (benutzerkonfigurierbare Gruppe)								
Anzahl der Nebenstellen in der Rufzuschaltungsgruppe	5	5	5	5	5	5	5	5
Gruppenruf, Sammelanschluss, Basic-MULAPs								
Summe der Gruppenrufe, Sammelanschlüsse, Basic-MULAPs, Chef-MULAPs und Sprachbox-Gruppen pro Kommunikationssystem	800	800	800	800	800	800	800	800
Länge des Gruppennamens	16	16	16	16	16	16	16	16
Anzahl der Gruppen, denen ein Benutzer zugewiesen werden kann	32	32	32	32	32	32	32	32
Teilnehmer pro Gruppenruf, Sammelanschluss, Basic-MULAP	20	20	20/32 ⁵⁰	20/32 ⁵⁰	20/32 ⁵⁰	20/32 ⁵⁰	32	32
Chef-MULAPs, Team-Gruppen, Top-Gruppen und Voicemail-Gruppen:								
Summe der Chef-MULAPs, Team- und Top-Gruppen pro	500	500	500	500	500	500	500	500
Teilnehmer pro Chef-MULAP, Team-Gruppe, Top-Gruppe	10	10	10	10	10	10	10	10
MULAP-Tasten pro Telefon	10	10	10	10	10	10	10	10

	X1W		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Voicemail-Gruppen								
Anzahl der Voicemail-Gruppen	20	20	20	20	20	20	20	20
Teilnehmer pro Sprachbox-Gruppe	20	20	20	20	20	20	20	20
Durchsage an Gruppe (Sprachdurchsage)								
Gleichzeitige Durchsagen pro Kommunikationssystem	1	1	1	1	1	1	1	1
Empfänger der Durchsage	20	20	20/32 ⁵⁰	20/32 ⁵⁰	20/32 ⁵⁰	20/32 ⁵⁰	32	32
UCD-Gruppen								
UCD-Gruppen pro System	60	60	60	60	60	60	60	60
Ansagen pro UCD-Gruppe	7	7	7	7	7	7	7	7
Prioritätsebenen pro UCD-Gruppe	10	10	10	10	10	10	10	10
Wartende Anrufe pro UCD-Gruppe (letzte Gruppe max. 72)	30	30	30	30	30	30	30	30
UCD-Agenten								
UCD-Agenten-IDs pro Kommunikationssystem	330	330	330	330	330	330	330	330
Gleichzeitig aktive UCD-Agenten pro Kommunikationssystem	64	64	64	64	64	64	64	64
UCD-Ansagen								
Anrufer pro Kommunikationssystem, denen gleichzeitig eine Ansage eingespielt werden kann	8	8	8	8	8	8	8	8

⁵⁰ Werte sind gestaffelt nach Board-Version: Basic/Advanced

Ausbaugrenzen und Kapazitäten

Tabelle 56: Daten für OpenScape Business S

	Basic Server (S)	Standard Server (S)	Advanced Server (S)
Anrufübernahmegruppen			
Anrufübernahmegruppen pro System	32	64	128
Teilnehmer pro Anrufübernahmegruppe	32	32	32
Rufzuschaltung (benutzerkonfigurierbare Gruppe)			
Anzahl der Nebenstellen in der Rufzuschaltungsgruppe	5	5	5
Gruppenruf, Sammelanschluss, Basic-MULAPs			
Summe der Gruppenrufe, Sammelanschlüsse, Basic-MULAPs, Chef-MULAPs und Sprachbox-Gruppen pro Kommunikationssystem	800	800	800
Länge des Gruppennamens	16	16	16
Anzahl der Gruppen, denen ein Benutzer zugewiesen werden kann	32	32	32
Teilnehmer pro Gruppenruf, Sammelanschluss, Basic-MULAP	32	32	32
Chef-MULAPs, Team-Gruppen, Top-Gruppen und Voicemail-Gruppen:			
Summe der Chef-MULAPs, Team- und Top-Gruppen pro	500	500	500
Teilnehmer pro Chef-MULAP, Team-Gruppe, Top-Gruppe	10	10	10
MULAP-Tasten pro Telefon	10	10	10
Voicemail-Gruppen			
Anzahl der Voicemail-Gruppen	20	20	20
Teilnehmer pro Sprachbox-Gruppe	20	20	20
Durchsage an Gruppe (Sprachdurchsage)			
Gleichzeitige Durchsagen pro Kommunikationssystem	1	1	1
Empfänger der Durchsage	20	20	20
UCD-Gruppen			
UCD-Gruppen pro System	60	60	60
Ansagen pro UCD-Gruppe	7	7	7
Prioritätsebenen pro UCD-Gruppe	10	10	10
Wartende Anrufe pro UCD-Gruppe (letzte Gruppe max. 72)	30	30	30
UCD-Agenten			

	Basic Server (S)	Standard Server (S)	Advanced Server (S)
UCD-Agenten-IDs pro Kommunikationssystem	330	330	330
Gleichzeitig aktive UCD-Agenten pro Kommunikationssystem	64	64	64
UCD-Ansagen			
Anrufer pro Kommunikationssystem, denen gleichzeitig eine Ansage eingespielt werden kann	8	8	8

26.4.8 Anruf-Routing

	X1W	X3W/R	X5W/R	X8	Server (S)
Leitweglenkung LCR					
Gewählte Ziffern	24	24	24	24	24
Geprüfte Ziffern	24	24	24	24	24
Wahlpläne (max. 10 Felder pro Plan)	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
Anzahl der Zeitzonen pro Tag/Woche	8	8	8	8	8
Ziffern pro Wahlregel	40	40	40	40	40
Nachtschaltung					
Berechtigte Teilnehmer pro System	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 System	64	64	64	64	64

Attendants für V2 Mainboards

	X1	X3W/R	X5W/R	X8	Server (S)
myAttendant					

Ausbaugrenzen und Kapazitäten

	X1	X3W/R	X5W/R	X8	Server (S)
myAttendant (UC Suite) pro System	-	20	20	20	20
AutoAttendant (UC Smart)					
Company Auto-Attendant	100	100	100	100	100
AutoAttendant (UC Suite)					
Automatischer Vermittlungsplatz (VPL)	-	20/ 20/ 0 ⁵¹	20/ 20/ 0 ⁵¹	20/ 20/ 0 ⁵¹	20
OpenScape Business Attendant					
OpenScape Business Attendants pro System	-	8	8	8	8

Attendants für V3 Mainboards

	X1W	X3W/R	X5W/R	X8	Server (S)
myAttendant					
myAttendant (UC Suite) pro System	4	4/20 ⁵²	4/20 ⁵²	20	20
AutoAttendant (UC Smart)					
Company Auto-Attendant	100	100	100	100	100
AutoAttendant (UC Suite)					
Automatischer Vermittlungsplatz (VPL)	20	20/ 20/ ⁵²	20/ 20 ⁵²	20/ 20 ⁵²	20
OpenScape Business Attendant					
OpenScape Business Attendants pro System	8	8	8	8	8

26.4.9 Multimedia Contact Center

	X1W	X3W/R	X5W/R	X8	Server (S)
Contact Center Warteschlangen					
Warteschlangen pro Kommunikationssystem	-	50	50	50	50
Nachbearbeitung					
Nachbearbeitungscodes	-	unbeschränkt	unbeschränkt	unbeschränkt	unbeschränkt
Agenten					

⁵¹ Werte sind gestaffelt nach UC Booster-Konfiguration: Booster Server / Booster Card / ohne UC Booster. Für V3 Mainboards ist der höchste Wert gültig.

⁵² Werte sind gestaffelt nach Board-Version: Basic/Advanced

	X1W	X3W/R	X5W/R	X8	Server (S)
(Agenten gleichzeitig aktiv)	-	64	64	64	64
Agenten (konfigurierbar)	-	192	192	192	192
Historische Berichte					
myReports Clients gleichzeitig aktiv pro System	-	1	1	1	1

26.4.10 Mobility Ausbaugrenzen

Tabelle 57: Daten für V2 OCC Mainboards

	X1	X3W/R	X5W/R	X8
Teleworker-Arbeitsplätze:				
Teleworker-Arbeitsplätze über VPN pro Kommunikationssystem	10	10	10	10
Mobility Teilnehmer:				
Mobility Entry-Teilnehmer pro System	30	150	150	150
myPortal to go (UC Smart): Teilnehmer pro System	30	150/ 150/ 50 ⁵³	150/ 150/ 50 ⁵³	150/ 150/ 50 ⁵³
myPortal to go (UC Suite): Teilnehmer pro System	-	150/ 150/ 0 ⁵³	150/ 150/ 0 ⁵³	150/ 150/ 0 ⁵³

Tabelle 58: Daten für V3 OCC Mainboards

	X1W		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
Teleworker-Arbeitsplätze:								
Teleworker-Arbeitsplätze über VPN pro Kommunikationssystem	10	10	10	10	10	10	10	10
Mobility Teilnehmer:								
Mobility Entry-Teilnehmer pro System	150/ 500 ⁵⁴	150/ 500 ⁵⁴	150	150/ 500 ⁵⁴	150/ 500 ⁵⁴	150/ 500 ⁵⁴	500	500

⁵³ Werte sind gestaffelt nach UC Booster-Konfiguration: Booster Server / Booster Card / ohne UC Booster

Ausbaugrenzen und Kapazitäten

	X1W		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
myPortal to go (UC Smart): Teilnehmer pro System	150	150	150/ 500 ⁵⁴	150/ 500 ⁵⁴	150/ 500 ⁵⁴	150/ 500 ⁵⁴	500	500
myPortal to go (UC Suite): Teilnehmer pro System	-	50	-	50/ 500 300 bei Contact Center	-	50/ 500 300 bei Contact Center	-	500 300 bei Contact Center
myPortal for Teams (UC Smart): Teilnehmer pro System	150	150	150/ 500 ⁵⁴	150/ 500 ⁵⁴	150/ 500 ⁵⁴	150/ 500 ⁵⁴	500	500
myPortal Team (UC Suite): Teilnehmer pro System	-	50	-	50/ 500 300 bei Contact Center	-	50/ 500 300 bei Contact Center	-	500 300 bei Contact Center

Tabelle 59: Daten für OpenScape Business S

	Basic Server (S)	Standard Server (S)	Advanced Server (S)
Mobility Teilnehmer:			
Mobility Entry-Teilnehmer pro System	50	150	150
myPortal to go (UC Smart): Teilnehmer pro System	50	250	500
myPortal to go (UC Suite): Teilnehmer pro System	50	250	500
myPortal for Teams (UC Smart): Teilnehmer pro System	50	250	500
myPortal for Teams (UC Suite): Teilnehmer pro System	50	250	500

26.4.11 Sicherheit

	X1W	X3W/R	X5W/R	X8	Server (S)
Individuelles Codeschloss					

⁵⁴ Werte sind gestaffelt nach Board-Version: Basic/Advanced

	X1W	X3W/R	X5W/R	X8	Server (S)
Ziffern pro Telefonschlosscode	5	5	5	5	5
Zulässige Zeichen	0 – 9	0 – 9	0 – 9	0 – 9	0 – 9
Amtsberechtigung					
Anzahl der Erlaubnislisten	6	6	6	6	6
Anzahl der Verbotslisten	6	6	6	6	6
Erlaubnisliste kurz (10 Einträge mit jeweils 32 Stellen)	5	5	5	5	5
Erlaubnisliste lang (100 Einträge mit jeweils 32 Stellen)	1	1	1	1	1
Verbotsliste kurz (10 Einträge mit jeweils 32 Stellen)	5	5	5	5	5
Verbotsliste lang (50 Einträge mit jeweils 32 Stellen)	1	1	1	1	1
Berechtigungsklassen					
Berechtigungsklassen pro System	15	15	15	15	15
Matrixgröße – Tag und Nacht – Anzahl der Amtsleitungen	30	30	30	30	30
Erlaubnis- und Verbotslisten	15	15	15	15	15
Geschlossene verwendete Gruppen (VBZ-Gruppen)					
VBZ-Gruppen) pro System	16	64	64	64	64
Matrixgröße – Tag und Nacht – Anzahl der Amtsleitungen	30	30	30	30	30
Erlaubnis- und Verbotslisten	15	15	15	15	15

26.4.12 Vernetzung von OpenScape Business

Vernetzung von OpenScape Business X1W, OpenScape Business X3R/X3W, OpenScape Business X5R/X5W, OpenScape Business X8, OpenScape Business S: Darüber hinausgehende Ausbaugrenzen für Vernetzungen können über projektspezifische Freigaben beantragt werden. Bitte beachten Sie die aktuelle Vertriebsfreigabe

Ausbaugrenzen und Kapazitäten

	X1W	X3W/R	X5W/R	X8	Server (S)
Vernetzung von OpenScape Business					
Vernetzte Kommunikationssysteme (Knoten)	8/ 32 ⁵⁵				
Teilnehmer im Netz	1000	1000	1000	1000	1000

26.4.13 Anschaltungen

Die folgenden Informationen gelten nur für Systeme mit V2 OCC Mainboards.

	X1	X3W/R	X5W/R	X8	Server (S)
OpenStage Gate View					
Kameras pro Kommunikationssystem	-	8/ 2/ 0 ⁵⁶	8/ 2/ 0 ⁵⁶	8/ 2/ 0 ⁵⁶	Nicht unterstützt
Telefone (OpenStage HFA 60, 60 G, 80, 80 G, 80 E) für die Darstellung des Kamerabilds pro Kommunikationssystem	-	20/ 10/ 0 ⁵⁶	20/ 10/ 0 ⁵⁶	20/ 10/ 0 ⁵⁶	Nicht unterstützt
iPhone Apps oder Web-Clients für die Darstellung des Kamerabilds pro Kommunikationssystem	-	20/ 10/ 0 ⁵⁶	20/ 10/ 0 ⁵⁶	20/ 10/ 0 ⁵⁶	Nicht unterstützt

26.4.14 Application Connectivity

Tabelle 60: Daten für V2 OCC Mainboards

	X1	X3W/R	X5W/R	X8
CSTA-Schnittstelle				
CSTA-Links via CSP pro System	-	4/ 4/ 0 ⁵⁷	4/ 4/ 0 ⁵⁷	4/ 4/ 0 ⁵⁷
Monitorpunkte für Amtsleitungen oder Teilnehmer	-	1500	1500	1500
TAPI 170 Middleware Server	-	4	4	4
TAPI 120 Clients (CSTA)	-	150/ 150/ 0 ⁵⁷	150/ 150/ 0 ⁵⁷	150/ 150/ 0 ⁵⁷
Web Services Interface (WSI)				

⁵⁵ Die Werte sind gestaffelt nach: Netzwerk mit UC Suite / Netzwerk ohne UC Suite

⁵⁶ Werte sind gestaffelt nach UC Booster-Konfiguration: Booster Server / Booster Card / ohne UC Booster

	X1	X3W/R	X5W/R	X8
WSI - gleichzeitig aktive Clients in Summe	30	500/ 300/ 150 ⁵⁷	500/ 300/ 150 ⁵⁷	500/ 300/ 150 ⁵⁷
myPortal @work	30	250/ 150/ 50 ⁵⁷	250/ 150/ 50 ⁵⁷	250/ 150/ 50 ⁵⁷
myPortal to go	30	150/ 150/ 50 ⁵⁷	150/ 150/ 50 ⁵⁷	150/ 150/ 50 ⁵⁷
DeskPhone CP 400/600/600E/ 700/700X/710 mit WSI	30	150/ 150/ 50 ⁵⁷	150/ 150/ 50 ⁵⁷	150/ 150/ 50 ⁵⁷
OpenScape Business Attendant	0	8/ 8/ 8 ⁵⁷	8/ 8/ 8 ⁵⁷	8/ 8/ 8 ⁵⁷
OpenScape Business BLF	0	150/ 150/ 50 ⁵⁷	150/ 150/ 50 ⁵⁷	150/ 150/ 50 ⁵⁷
Application Launcher	30	250/ 150/ 50 ⁵⁷	250/ 150/ 50 ⁵⁷	250/ 150/ 50 ⁵⁷
TAPI 120 (WSI-Modus)	30	0/ 0/ 30 ⁵⁷	0/ 0/ 30 ⁵⁷	0/ 0/ 30 ⁵⁷
Anwendung von Drittanbietern	Rest	Rest	Rest	Rest

Tabelle 61: Daten für V3 OCC Mainboards

	X1W		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
CSTA-Schnittstelle								
CSTA-Links via CSP pro System	-	-	4	4	4	4	4	4
Monitorpunkte für Amtsleitungen oder Teilnehmer	1650	1650	1650/ 3750 ⁵⁸	1650/ 3750 ⁵⁸	1650/ 3750 ⁵⁸	1650/ 3750 ⁵⁸	3750	3750
TAPI 170 Middleware Server	4	4	4	4	4	4	4	4
TAPI 120 Clients (CSTA)	150	150	150/ 500 ⁵⁸	150/ 500 ⁵⁸	150/ 500 ⁵⁸	150/ 500 ⁵⁸	500	500
Web Services Interface (WSI)								
WSI - gleichzeitig aktive Clients in Summe	150	300	150/ 500 ⁵⁸	300/ 1000 ⁵⁸	150/ 500 ⁵⁸	300/ 1000 ⁵⁸	1000	1000
myPortal @work	150	150	150/ 250 ⁵⁸	150/ 250 ⁵⁸	150/ 250 ⁵⁸	150/ 250 ⁵⁸	250	250

⁵⁷ Werte sind gestaffelt nach UC Booster-Konfiguration: Booster Server / Booster Card / ohne UC Booster

Ausbaugrenzen und Kapazitäten

	X1W		X3W/R		X5W/R		X8	
		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD		+ NVMe SSD
myPortal to go	150	150	150/ 500 ⁵⁸	150/ 500 ⁵⁸	150/ 500 ⁵⁸	150/ 500 ⁵⁸	500	500
myPortal for Teams	150	150	150/ 500 ⁵⁸	150/ 500 ⁵⁸	150/ 500 ⁵⁸	150/ 500 ⁵⁸	500	500
DeskPhone CP 400/600/600E/ 700/700X/710 mit WSI	150	150	150/ 500 ⁵⁸	150/ 500 ⁵⁸	150/ 500 ⁵⁸	150/ 500 ⁵⁸	500	500
OpenScape Business Attendant	8	8	8	8	8	8	8	8
OpenScape Business BLF	150	150	150	150	150	150	150	150
Application Launcher	150	150	150/ 500 ⁵⁸	150/ 500 ⁵⁸	150/ 500 ⁵⁸	150/ 500 ⁵⁸	500	500
TAPI 120 (WSI- Modus)	Anmerkung: Produktauslauf auf V3 OCC Mainboards. In V3 nur für V2 Mainboards unterstützt.							
Anwendung von Drittanbietern	Rest	Rest	Rest	Rest	Rest	Rest	Rest	Rest

Tabelle 62: Daten für OpenScape Business S

	Basic Server (S)	Standard Server (S)	Advanced Server (S)
CSTA-Schnittstelle			
CSTA-Links via CSP pro System	4	4	4
Monitorpunkte für Amtsleitungen oder Teilnehmer	3750	3750	3750
TAPI 170 Middleware Server	4	4	4
TAPI 120 Clients (CSTA)	50	500	1500
Web Services Interface (WSI)			
WSI - gleichzeitig aktive Clients in Summe	150	500	1500
myPortal @work	50	250	500
myPortal to go	50	250	500

⁵⁸ Werte sind gestaffelt nach Board-Version: Basic/Advanced

	Basic Server (S)	Standard Server (S)	Advanced Server (S)
myPortal for Teams	50	250	500
DeskPhone CP 400/600/600E/ 700/700X/710 mit WSI	50	250	500
OpenScape Business Attendant	8	8	8
Application Launcher	50	250	500
TAPI 120 (WSI-Modus)	0	0	0
Anwendung von Drittanbietern	Rest	Rest	Rest

26.4.15 Gebührenabrechnung

	X1W	X3W/R	X5W/R	X8	Server (S)
Gesprächsdatenerfassung zentral					
Einträge im Gesprächsdatenpuffer pro System	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	0-9	0-9	0-9	0-9	0-9

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	<p>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.</p> <p>Beispiel: Grundeinstellungen > System > System Flags</p>
Registerkarte	<p>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.</p> <p>Beispiel:</p> <ul style="list-style-type: none">• Statische IP Adresse hinzufügen• Statische IP Adresse ändern• Statische IP Adresse löschen
Bereich	<p>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.</p>

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:

- **Laden der Audio-Dateien via HTTP**

Parameter	Beschreibung
Laden der Audio-Dateien via HTTP	
Ansagedatei	Auswählen der WAV-Datei mit der Ansage vom lokalen Dateisystem auswählen. Dateiformat: siehe Hinweis im WBM.
Bereits geladene Audio-Dateien	
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:

- **Laden der Audio-Dateien via HTTP**

Parameter	Beschreibung
Laden der Audio-Dateien via HTTP	
Ansagedatei	Auswählen der WAV-Datei mit der Ansage vom lokalen Dateisystem auswählen. Dateiformat: siehe Hinweis im WBM.
Bereits geladene Audio-Dateien	
WAV-Datei	Anzeige der im Kommunikationssystem geladenen Ansagedateien
Löschen	Löschen der Ansagedatei

Parameter	Beschreibung
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.
Maßnahme	Export einer gezippten XML-Datei (z.B. für Bearbeitung in Excel) mit folgenden Daten: Name, Rufnummer des Teilnehmers, Durchwahlnummer, Teilnehmertyp, Lizenzen, Gruppen/Sammelanschlüsse (nicht Team/Top), virtuelle Teilnehmer, Leitungen, Leitungsgruppen, Voicemail.

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 Sprachbox-Rufnummer.
Name	Anzeige des Namens der Sprachbox.
Meldungen	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.
Name	Anzeige des Namens der Sprachbox.
Kennwörter zurücksetzen	Ist dieses Flag aktiviert, wird das Passwort der Sprachbox auf das Standardpasswort 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	
Meldungen	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.
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:

- **Begrüßungen**

Parameter	Beschreibung
Begrüßungen	
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.

Experten-Modus

Parameter	Beschreibung
Laden	<p>Eine zuvor gespeicherte Begrüßung oder eine Wave-Datei wird in die SmartVM geladen. Die zu ladende Wave-Datei muss folgendes Format haben:</p> <p>PCM, 16 bit, 8khz, mono</p> <p>Beim Laden wird die ausgewählte Wave-Datei konvertiert. Je nach Größe der Wave-Datei kann dies einige Zeit in Anspruch nehmen.</p>
Backup	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:

- **Wiederherstellen**

Parameter	Beschreibung
Wiederherstellen	
Meldungen	<p>Überschreibt nicht nur die Begrüßungen der ausgewählten Sprachboxen, sondern auch die Nachrichten.</p> <p>Standard: Deaktiviert.</p>
Aufschalten	<p>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.</p> <p>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.</p> <p>Standard: Deaktiviert.</p>
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.

Parameter	Beschreibung
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
Web-Server-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.
Kennwort	Passwort für die Anmeldung am Software-Server.

Experten-Modus

Parameter	Beschreibung
Software Update-Information	Aktivierung der Abfrage, ob am Software-Server eine neue Software-Version bereitgestellt ist.
Startzeit	Zeitpunkt der Abfrage. Wertebereich: 00.00 bis 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.
Kennwort	Passwort für die Anmeldung am Proxy-Server.
Spezielle statische Route verwenden	Für Kunden mit einer WAN-Verbindung für SIP-Trunks ohne Internet-Datenvolumen kann die Funktion Spezielle statische Route verwenden verwendet werden, um ein Software-Update der OSBiz über eine alternative LAN-Schnittstelle durchzuführen. Die dynamische IP-Adresse des Update-Servers wird automatisch ermittelt und steht dann für diesen Vorgang als Routing-Eintrag zur Verfügung. Um diese Option zu nutzen, gehen Sie bitte wie folgt vor: <ul style="list-style-type: none"> • Aktivieren Sie das Flag Spezielle statische Route verwenden, und
Spezielle statische Route für Software-Update via LAN-Interface	
Gateway IP-Adresse der Route	konfigurieren Sie die IP-Adresse des Standard-Gateways der LAN-Schnittstelle, über die eine Verbindung zum Internet möglich ist, als Gateway-IP-Adresse der Route.
Letzter Software Update	Anzeige, wann das letzte Software-Update durchgeführt wurde.
Schaltflächen	
Standard	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	

Parameter	Beschreibung
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	
Version	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.

Experten-Modus

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 Systemteletyps, 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 Teletyps übertragen.
Dateiname	Anzeige des Dateinamens der Image-Datei.

Parameter	Beschreibung
Gerätetyp	Anzeige des Systemteletyp, der zur Image-Datei gehört.
Version	Anzeige der Version der Image-Datei.
Type	Typ des Systemtelefons.
Standard	Als Default 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**

Wenn der Benutzer ein Deskshare-Benutzer ist, ist das Kontrollkästchen ausgegraut, so dass Sie ein Gerät nicht für diesen Benutzer bereitstellen können.

Parameter	Beschreibung
Aktuell installierte Images	
Rufnr	Rufnummer des Systemtelefons.
Gerätetyp	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	

Experten-Modus

Parameter	Beschreibung
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 Systemteletyp 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
Basisstationsdaten	

Parameter	Beschreibung
BS-Frequenz	Zeigt die Frequenzen der ausgewählten Basisstation an. Es können bis zu 10 verschiedene Frequenzkanäle gleichzeitig ausgewählt werden (siehe nachfolgende Tabelle).
Basistation	Nummer der Basisstation.
SW-Version	Software-Version der Basisstation.
HW Version	Hardware-Version der Basisstation.
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 SLC. Gezählt wird bei der neuen Basisstation.
Inter SLC Handover	Anzahl der Handover-Vorgänge zwischen SLC-Baugruppen. Gezählt wird bei der neuen Basisstation.
SLC-weit	
Lost Calls	Anzahl von Gesprächen, die aus Ressourcen Gründen nicht vermittelt werden konnten.

Parameter	Beschreibung
SLMUC Overload	Anzahl der Overload-Situationen auf der Baugruppe SLC. Die Anzahl der freien Poolelemente auf der SLC-Baugruppe unterschreitet einen Minimalwert. Alle kommenden Belegungen werden von der IWU der SLC 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.
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:

- **Baugruppenstatus**

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.
Anhalten	Aktualisierung der Anzeige wird gestoppt.

27.2.4.2 Port / Baugruppen Zustand > Out of Service

Parameterbeschreibung der Registerkarten:

- **Port außer Betrieb**
- **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.

Parameter	Beschreibung
Status	<p>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 außer Betrieb durch Tool sein, d.h. dass sie über Baugruppe sperren gesperrt wurden.</p> <p>Der Zustand in Betrieb ist nicht identisch mit aktiv. Der Port-Status kann beispielsweise aktiv, in Betrieb oder auch inaktiv, in Betrieb sein.</p>
Schaltflächen	
Auswahl sperren	<p>Die markierten Ports werden gesperrt.</p> <p>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.</p>
Auswahl freigeben	Die markierten Ports werden freigegeben.
Baugruppe sperren	<p>Die markierten Baugruppen und deren Ports werden gesperrt.</p> <p>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.</p>
Baugruppe freigeben	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-Konfiguration ändern**

Parameter	Beschreibung
In der Trace-Ausgabe enthaltene Header-Daten	
Globale Trace-Header Format-Einstellungen	<p>Bei aktiviertem Flag können die Optionen für die nachfolgenden Header-Daten aktiviert oder deaktiviert werden.</p> <p>Standardwert: Aktiviert</p>

Parameter	Beschreibung
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
Uhrzeit	Bei aktiviertem Flag ist die Zeitangabe in der Trace-Ausgabe enthalten. Standardwert: Aktiviert
Modulname	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
Aufbereitung der Trace-Daten	
Volle Formatierung mit Parameterexpansion (Standard)	Standard Ausgabe-Modus: Alle Datentypen werden erweitert. 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.
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**

Tipp: 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 S₀-, 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:

- **Anzeige**
- **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-Komponenten starten/stoppen**

Parameter	Beschreibung
Paketname	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).

Anmerkung: Das Aufzeichnen von Gesprächen und Verbindungsdaten ist ein Straftatbestand, 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

Parameter	Beschreibung
Datei mit dem Zertifikat (PEM oder Binär-Format)	<p>Auswahl der X.509-Datei, die das in das Kommunikationssystem zu importierende Zertifikat beinhaltet.</p> <p>Nach Auswahl der X.509-Datei kann der Fingerabdruck des zu importierenden Zertifikats angezeigt und anschließend das Zertifikat in das Kommunikationssystem importiert werden.</p> <p>INFO: Das Importieren des Zertifikats sollte nach der Prüfung des Fingerabdrucks erfolgen.</p>

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 Deaktivierungszeitpunkt	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

Parameter	Beschreibung
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 > 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
Allgemeines	
Trace-Level	Trace-Detailtiefe (Trace-Level 0 = niedrigste Detailtiefe bis Trace-Level 4 = höchste 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

Parameter	Beschreibung
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.

27.2.5.11 Traces > Call Supervision

Mit dieser Funktion kann die Überwachung von Leitungs- und Teilnehmerschnittstellen gestartet und gestoppt werden.

Parameterbeschreibung der Registerkarten:

- **Protokoll starten/stoppen**
- **Anzeige**
- **Laden über HTTP**

Parameter	Beschreibung
Ausgewählter Port	Leitungs- oder Teilnehmerschnittstelle für die die Anrufüberwachung gestartet oder gestoppt werden soll.
Nr.	Fortlaufende Nummer.
Uhrzeit	Uhrzeit des Events (Ereignisses).
Callnumber/Access	Rufnummer und physikalische Schnittstelle.

Parameter	Beschreibung
Status	<p>Zustand der Schnittstelle.</p> <p>Möglich sind folgende Schnittstellenzustände:</p> <ul style="list-style-type: none"> • 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.) • Fehler (Fehlerstatus) • 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) • Unbekannter Zustand

Parameter	Beschreibung
Ereignis	<p>Ereignis</p> <p>Möglich sind folgende Events:</p> <ul style="list-style-type: none"> • 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	<p>Bei aktiviertem Flag erfolgt eine automatische Aktualisierung der Anzeige der Anrufüberwachung.</p> <p>Standardwert: Aktiviert</p>
Sekunden bis zur nächsten Aktualisierung	<p>Zeit in Sekunden nach deren Ablauf eine Aktualisierung der Anrufüberwachung erfolgt.</p>

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
Paketname	Name der Lizenz-Trace-Komponente.
Trace-Level	<p>Definition der Detailtiefe der Aufzeichnung der Lizenz-Trace-Komponente</p> <p>Standardwert: Standard</p>

Parameter	Beschreibung
Trace-Level: niedrig	Niedrige Detailtiefe für die Trace-Aufzeichnung.
Trace-Level: Standard	Mittlere Detailtiefe für die Trace-Aufzeichnung.
Trace-Level: Alle	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
Profil-Name	Name des Trace-Profiles
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-Komponenten starten/stoppen**
- **Standard-Trace-Einstellungen**

Parameter	Beschreibung
Subsystem-Name	Name der Trace-Komponente
Trace-Komponenten-Index	Fortlaufende Nummer
Trace-Level	Trace-Detailtiefe (Trace-Level 0 = niedrigste Detailtiefe bis Trace-Level 9 = höchste 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-Dump**

Parameter	Beschreibung
TCP-Dump starten	Startet den TCP-Dump
Start-Parameter	
Schnittstellename	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 bis 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

Parameter	Beschreibung
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.

Anmerkung: 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

27.2.5.17 Traces > Kernel-Crash-Daten

Der Kernel Crash-Datendienst dient der automatischen Erfassung von Kernel-Crash-Daten. Er ist nur auf OSBiz X-Systemen mit V3-Mainboards verfügbar: OCCLA, OCCMA(R), OCCMB(R).

Der Dienst erfordert einen Speicherplatz von 200 MB. Die betroffenen Festplatten sind:

- SATA SSD 16GB (wenn keine NVMe SSD eingebaut ist)

- NVMe SSD

Es wird empfohlen, die Traces vor dem Start des Dienstes zu löschen, wenn Sie Speicherplatz freigeben möchten. Wenn der Platz nicht ausreicht, wird der Dienst keine Daten erfassen.

Parameterbeschreibung der Registerkarten:

- **Kernel-Crash-Daten**

Parameter	Beschreibung
Kernel Crash-Datendienst	Status des Dienstes: Grün: Der Dienst ist aktiviert. Grau: Der Dienst ist deaktiviert.
Start	Startet den Kernel Crash-Datendienst.
Anhalten	Stoppt den Kernel Crash-Datendienst.

Beim Starten oder Stoppen des Kernel Crash-Datendienstes wird automatisch ein Neustart des Systems eingeleitet. Der Dienst behält seinen Status nach dem Neustart des Systems bei.

Wenn der Dienst aktiviert ist, sind nach einem Systemneustart mit dem Grund WATCHDOG oder KERNEL_OOPS Kernel-Crash-Daten im oso-Diagnosespeicher verfügbar. Um Kernel-Crash-Daten zu sammeln, muss das Kontrollkästchen **CoreLog Protocol** unter **Servicezentrum > Diagnostik > Rückverfolgung > Diagnose-Protokolle** aktiviert sein.

Nach dem Sammeln der Kernel-Crash-Daten muss der Dienst manuell deaktiviert werden.

27.2.5.18 Traces > Medienserver-Trace

Anhand von Medienserver-Trace werden die Prozess- und Zustandsinformationen einzelner Medienserver-Komponenten des Kommunikationssystems aufgezeichnet.

Parameterbeschreibung der Registerkarten:

- **Trace-Komponente des Medienservers bearbeiten**

Parameter	Beschreibung
Package-Name	Name der Trace-Komponente Standardwert: Media Server
Trace-Level	Detaillierungsgrad des Trace (None, Unspecified, Default, Fatal, Error, Warning, Info, Unexpected, Debug, Fine, Finest)
Trace-Status	Status des Trace: Grün: Der Trace ist aktiviert. Grau: Der Trace ist deaktiviert.
Start	Startet den Medienserver-Trace.

Parameter	Beschreibung
Anhalten	Stoppt den Medienserver-Trace.

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
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 Ereignisse > 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.
Empfänger von Notfallbenachrichtigungen	
Empfänger für Notfälle	E-Mail-Adresse eines Sicherheitsbeauftragten vor Ort, an den eine E-Mail gesendet wird, wenn eine Notrufnummer gewählt 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 zurücksetzen**
- **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 senden	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.

Experten-Modus

Parameter	Beschreibung
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: <ul style="list-style-type: none">• 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	<p>Kontrollierter Restart (Neustart) von OpenScape Business:</p> <ul style="list-style-type: none"> • 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).

Parameter	Beschreibung
System-Reload ausführen	<p>Reload von OpenScape Business:</p> <ul style="list-style-type: none"> • 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	<p>Kontrolliertes Herunterfahren von OpenScape Business X:</p> <ul style="list-style-type: none"> • 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	<p>Definition einer PIN für die Aktivierung des Shutdowns (das kontrollierte Herunterfahren des Kommunikationssystems) über ein Systemtelefon</p>
Application Board neu starten	<p>Kontrollierter Restart (Neustart) des Application Boards OCAB inklusive der UC Applikation (UC Smart oder UC Suite):</p> <p>Bei einem Restart des Application Boards OCAB werden die Verbindungen zu allen aktiven Anwendungen, wie zum Beispiel myPortal for Desktop und myAttendant, getrennt. Nach dem Hochlauf werden alle Verbindungen automatisch wiederhergestellt.</p>
Applikationen	
Sync-Netzwerk	<p>Synchronisierung vernetzter Kommunikationssysteme:</p> <p>Nach der Änderung von Rufnummern, Durchwahlnummern oder Namen werden durch eine Synchronisierung die Daten in allen vernetzten Kommunikationssystemen aktualisiert.</p>
UC Application neu starten	<p>Kontrollierter Restart (Neustart) der UC Applikation (UC Smart oder UC Suite):</p> <p>Bei einem Restart der UC Applikation werden die Verbindungen zu allen aktiven Anwendungen, wie zum Beispiel myPortal for Desktop und myAttendant, getrennt. Nach dem Hochlauf werden alle Verbindungen automatisch wiederhergestellt.</p>

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.
Type	Auswahl des Typs.
Typ: Lesende Community	Kommunikationspartner mit lesendem SNMP-Zugang.
Typ: Lesende 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 1 = Software • 2 = Hardware
Enterprise	(nicht benutzt)
Uhrzeit	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 das Admin.-Protokoll des Kommunikationssystems. Das Admin-Protokoll bietet die Möglichkeit zu erfahren, wann Änderungen am Kommunikationssystem durchgeführt worden sind und von wem diese gemacht wurden. Protokolliert werden 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 Protokolldateien 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: <ul style="list-style-type: none"> • Gesamtes Protokoll: Die gesamten vorhandenen Systemtrace-Protokolldateien werden heruntergeladen. • Protokoll von heute: System Trace-Protokolldateien des heutigen Tages (ab 00:00 Uhr) werden heruntergeladen. • Eigene Auswahl: Von: XXX Bis: YYY: Die System Trace-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
Lizenz-Protokolle	Bei aktiviertem Flag werden Protokolldateien mit Meldungen über lizenzierungspflichtige Komponenten des Kommunikationssystems heruntergeladen. Standardwert: Aktiviert

Parameter	Beschreibung
Kunden-Trace	<p>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.</p> <p>Standardwert: Aktiviert</p>
Framework-Protokoll	<p>Bei aktiviertem Flag werden Protokolldateien mit Meldungen des WBM heruntergeladen.</p> <p>Standardwert: Aktiviert</p>
Diagnose-Protokoll	<p>Bei aktiviertem Flag werden Diagnose-Protokolle des Kommunikationssystems heruntergeladen.</p> <p>Standardwert: Aktiviert</p>
UC Suite-Protokolle	<p>Bei aktiviertem Flag werden Protokolldateien mit Meldungen der UC Suite (UC Suite-, CSP- und MEB-Protokolle) heruntergeladen. Folgende Auswahlmöglichkeiten bestehen:</p> <ul style="list-style-type: none"> • 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. <p>Alle Protokolldateien werden in einer komprimierten Datei zusammengefasst. Für die OpenScape Business-Protokolle gelten folgende Dateibezeichnungen: UC Suite-Protokolldateien = vs_ jjj_ mm_ tt.log, CSP-Protokolldateien = csprtrace_ jjj_ mm_ tt.log, MEB-Protokolldateien = mebtrace_ jjj_ mm_ tt.log</p> <p>Standardwert: Deaktiviert</p>
Applikationsprotokolle	<p>Bei aktiviertem Flag werden Protokolldateien mit Meldungen des Applikationsanteils des Kommunikationssystems (zum Beispiel CSP-Protokolle) heruntergeladen.</p> <ul style="list-style-type: none"> • Gesamtes Protokoll: Alle vorhandenen Protokolldateien werden heruntergeladen. • Protokoll von heute: Protokolldateien des heutigen Tages (ab 00:00 Uhr) werden heruntergeladen. • Eigene Auswahl: Von: XXX Bis: YYY: Protokolldateien des ausgewählten Zeitraums werden heruntergeladen. <p>Alle Protokolldateien werden in einer komprimierten Datei zusammengefasst.</p> <p>Standardwert: Deaktiviert</p>
System-Diagnose-Protokolle	<p>Bei aktiviertem Flag werden Diagnose-Protokolle des Kommunikationssystems heruntergeladen.</p> <p>Standardwert: Aktiviert</p>

Experten-Modus

Parameter	Beschreibung
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 > Manuelle Aktionen > DLI-Wartung

Parameterbeschreibung der Registerkarten:

- **DLI-Gerätewartung**

Parameter	Beschreibung
Gerät löschen	Wählen Sie das Systemtelefon aus, das gelöscht werden soll. Mit dieser Aktion wird das Systemtelefon aus der DLI-Datenbank gelöscht. <hr/> Anmerkung: Vor einer DLI-Wartungsaktion (Löschen) müssen Sie sich vergewissern, dass das Gerät nicht mehr verwendet wird. <hr/>
Rufnr	Rufnummer des Systemtelefons.
Gerätetyp	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.

27.2.10.3 Aktionen > Automatische Aktionen > Garbage Collection

Parameterbeschreibung der Registerkarten:

- **Aktion ändern**
- **Action 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

Parameter	Beschreibung
Startzeit nach Mitternacht	Zeitpunkt nach Mitternacht, an dem die Aktion Garbage Collection durchgeführt wird. Beispiel: 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

27.2.10.4 Aktionen > Automatische Aktionen > DLS Notification

Parameterbeschreibung der Registerkarten:

- **Aktion ändern**
- **Action 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
Kennwort	Passwort für die Anmeldung am externen DLS-Server

27.2.10.5 Aktionen > Automatische Aktionen > SDHC-Integritätsprüfung

Parameterbeschreibung der Registerkarten

- SDHC-Integritätsprüfung

Parameter	Beschreibung
SDHC-Integritätsprüfung	
Integritätsprüfung starten	Aktiviert die sofortige Integritätsprüfung der Karte.

Parameter	Beschreibung
Integritätsprüfung starten aktiv	Aktiviert einen geplanten Tag, Monat, ein geplantes Jahr und eine geplante Uhrzeit für die Integritätsprüfung der Karte.
Protokoll-Datei	Das Ergebnis der letzten Dateiprüfungen wird ausgegeben.
Status/Empfohlene Aktion	Empfiehl Aktionen für jede Integritätsprüfung der Karte.

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.

27.2.12.4 Applikat.-Diagnose > Entwickler-Einstellungen > SIP-Provider-Profile

Parameterbeschreibung der Tags:

- SIP-Provider-Profil hinzufügen
- SIP-Provider-Profile bearbeiten

Diese Seite ist für die Verwendung durch geschultes Fachpersonal während der Zertifizierung eines neuen ITSP vorgesehen. Bitte lesen Sie die Dokumente im Unify-Wiki: <http://wiki.unify.com/index.php/>

Collaboration_with_VoIP_Providers#How_to_get_a_new_VoIP_provider_relea
um weitere Informationen zu erhalten.

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
Type	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 Tastendrucke 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) einzurichten.

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
Rufweitschaltung nach AUL zum externen Ziel	Bei aktiviertem Flag gilt: Ist das externe Anrufumleitungsziel nicht erreichbar, erfolgt eine Rufweitschaltung 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
Aufmerksamkeitssignale bei AUN-Gruppen	Bei aktiviertem Flag wird ein Anruf für ein Mitglied einer Anrufübernahmegruppe bei den anderen Gruppenmitgliedern optisch (Display) signalisiert. Wird der Anruf nicht innerhalb von vier Rufzyklen (4 x 5 Sekunden) angenommen, erhalten die anderen Gruppenmitglieder zusätzlich einen Hinweis. 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
Endgerätetausch erlaubt	Bei aktiviertem Flag können Systemtelefone ohne Veränderung der logischen Konfiguration (Rufnummer, Name, Tastenprogrammierung usw.) physikalisch umgesteckt werden (Relocate/Rufnummerntausch). Standardwert: Deaktiviert

Experten-Modus

Parameter	Beschreibung
Mehr als 1 externer Konferenzteilnehmer	<p>Bei aktiviertem Flag können mehrere externe Teilnehmer an einer Konferenz teilnehmen.</p> <p>Standardwert: Aktiviert</p>
automatisches Leitungsvormerken	<p>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.</p> <p>Standardwert: Deaktiviert</p>
Wahlwiederholung mit PKZ	<p>Bei aktiviertem Flag wird bei der Wahlwiederholung neben der Rufnummer auch eine vorher eingegebene PKZ wiederholt.</p> <p>Standardwert: Deaktiviert</p>
Automatische Leitungsbelegung	<p>Wenn dieses Flag aktiviert ist, so erfolgt mit Wahl einer Ziffer von einem Systemfernsprecher sofort eine Leitungsbelegung, und die gewünschte Rufnummer wird gewählt. Die Wahl der Zugangskennziffer ist dabei nicht erforderlich. Für die Anwahl eines internen Teilnehmers muss entweder</p> <ul style="list-style-type: none"> • die Taste Intern betätigt, und die Teilnehmerrufnummer nachgewählt werden • oder die entsprechende DSS-Tasten betätigt werden. <p>Diese Funktion ist nur dann verfügbar, wenn nur eine Richtung (siehe "Richtungen") konfiguriert ist.</p> <p>Sind im Kommunikationssystem noch Entry, ISDN oder a/b-Telefone angeschaltet, ist LCR mit automatischer Wahl nicht möglich.</p>
Nur eingerichtete Nummer für MSN benutzen	<p>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).</p> <p>Standardwert: Deaktiviert</p>
Wegeoptimierung	<p>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) an 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.</p> <p>Standardwert: Aktiviert</p>
DTMF automatisch	<p>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.</p> <p>Standardwert: Aktiviert</p>

Parameter	Beschreibung
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
Euroimpedanz	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 - 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 - 6 dBr, Relativer Pegel D/A = -1 - 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 Rufweitschaltungen 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 eingehenden Anruf von 6671234 wird im Display 023026671234 angezeigt. Standardwert: Deaktiviert

Experten-Modus

Parameter	Beschreibung
Leitungswechsel bei Direktruf	<p>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.</p> <p>Standardwert: Deaktiviert (nicht für USA, Kanada), Aktiviert (nur für USA, Kanada)</p>
Automatische Wahlwiederholung	<p>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.</p> <p>Standardwert: Deaktiviert</p>
Knoten-Rufnummer bei Voice Mail	<p>Bei aktiviertem Flag wird bei vernetzten Kommunikationssystemen definiert, ob die Knoten-Rufnummer bei der Identifizierung eines zentralen oder mehrerer dezentraler VoiceMail-Server mitzuliefern ist. Die Knotenrufnummer muss für die Identifizierung des oder der VoiceMail-Server mitgeliefert werden.</p> <p>Standardwert: Deaktiviert</p>
Anrufübernahme nach Wiederanruf	<p>Bei aktiviertem Flag werden Wiederanrufe und Rückrufe auch bei den anderen Mitgliedern einer Anrufübernahmegruppe signalisiert und können von diesen übernommen werden.</p> <p>Standardwert: Deaktiviert</p>
Einstellbare CLIP	<p>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.</p> <p>Standardwert: Aktiviert</p>
Anruferliste beim Zienteilnehmer im Falle Umleitung MULAP	<p>Bei aktiviertem Flag werden bei einer Umleitung MULAP kommende Anrufe in der Anruferliste des Zienteilnehmers eingetragen.</p> <p>Standardwert: Deaktiviert</p>

Parameter	Beschreibung
Rufweitchaltung nach Deflect call / Single step transfer	<p>Bei aktiviertem Flag gilt: Hat ein Teilnehmer eine Anrufumleitung zu einem internen Ziel aktiviert (Deflect Call), wird der Anruf bei diesem Ziel signalisiert. Nach abgelaufener Rufweitchaltungszeit 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. Das erste eingetragene Ziel in der Rufzielliste von Teilnehmer B ist Teilnehmer C und das zweite Ziel Teilnehmer D. Der Anruf wird bei Teilnehmer C und nach abgelaufener Rufweitchaltungszeit 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.</p> <p>Damit dieses Flag eine Wirkung hat, erfolgen die Umleitungsfunktion bei Anruf, Deflect und Single Step Call Transfer, und gelten vor allem für Anrufe, die über UC (Auto Attendant/ UCD-Gruppen) abgewickelt werden und bei denen diese Umleitungsfunktionen anwendbar sind.</p> <p>Standardwert: Aktiviert</p>
Ermittlung des Ziels über Rufzielliste beim Deflect call / Single step transfer	<p>Bei aktiviertem Flag gilt: Hat ein Teilnehmer eine Anrufumleitung zu einem internen Ziel aktiviert (Deflect Call) wird der Anruf bei diesem Ziel signalisiert und nach abgelaufener Rufweitchaltungszeit bei einem in der Rufzielliste eingetragenen weiteren Ziel. Beispiel: Für Teilnehmer A wurde ein Deflect Call auf Teilnehmer B ausgeführt. Das erste eingetragene Ziel in der Rufzielliste von Teilnehmer B ist Teilnehmer C. Nach abgelaufener Rufweitchaltungszeit wird der Anruf bei Teilnehmer C signalisiert.</p> <p>Damit dieses Flag eine Wirkung hat, erfolgen die Umleitungsfunktion bei Anruf, Deflect und Single Step Call Transfer, und gelten vor allem für Anrufe, die über UC (Auto Attendant/ UCD-Gruppen) abgewickelt werden und bei denen diese Umleitungsfunktionen anwendbar sind.</p> <p>Standardwert: Aktiviert</p>
Hinweiston während Sprachaufzeichnung	<p>Wenn das Flag aktiviert ist, gilt für OpenScape Business X: Wird während eines Gesprächs die Sprachaufzeichnung (Live Call Record) aktiviert, so wird bei aktiviertem Flag ein entsprechender Hinweiston ausgegeben.</p> <p>Standardwert: Aktiviert</p>

Parameter	Beschreibung
<p>E.164 Nummerierung</p>	<p>Über dieses Flag kann die Vernetzung der KDS von ortsübergreifenden oder weltweit aufgestellten Kundenanlagen ein- bzw. ausgeschaltet werden. Die Teilnehmer sind über eine öffentliche Rufnummer, d.h. die E.164-Rufnummer im nationalen oder internationalen Format (z.B. interne Calling Party Number im ISDN Format), erreichbar, ohne dass eine Knotenrufnummer vorgewählt werden muss. Jeder Teilnehmer repräsentiert sich mit seiner E.164 Rufnummer, die in optimierter Form dargestellt werden kann. Bei eingeschaltetem Flag wird die interne Rufnummer im E.164-Format übertragen.</p> <p>Ist dieses Flag gesetzt, so werden SIP-Teilnehmer mit der E.164-Langrufnummer (Standortnummer + interne Rufnummer z.B. 4923026673665) registriert.</p> <p>Standardwert: Deaktiviert</p>
<p>Erweiterte Schlüsselfunktionen</p>	<p>Wenn das Flag aktiviert ist – und nachdem eine beliebige Taste als "Shift-Taste" definiert wurde –, können auf der dann verfügbaren zweiten Tastenebene ausschließlich Rufnummern ohne LED-Unterstützung gespeichert werden. Beliebige Tastenfunktionen auf der ersten Tastenebene können programmiert werden. Die LED-Signalisierung gilt ausschließlich für die erste Tastenebene.</p> <p>Standardwert: Deaktiviert</p>
<p>A-Rufnummer in AUN-Gruppen / Rufzuschaltung / Umleitungsziel / RWS-Ziel</p>	<p>Bei aktiviertem Flag werden ob Rufnummer und Name eines Anrufers bei allen Mitgliedern einer Anrufübernahmegruppe, bei zugeschalteten Teilnehmern (Rufzuschaltung) und bei Umleitungs- und Rufweichtschaltungszielen angezeigt. Rufnummer und Name werden im Display angezeigt.</p> <p>Standardwert: Aktiviert</p>
<p>SPE Unterstützung</p>	<p>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.</p> <p>Standardwert: Deaktiviert</p> <hr/> <p>Anmerkung: Wenn Sie den Cloud-Dienst Unify Video verwenden möchten, muss die SPE-Unterstützung deaktiviert werden, um die Leitung zu registrieren, es sei denn, es wurde ein SPE-Zertifikat in das System importiert.</p> <hr/>

Parameter	Beschreibung
SPE Advisory Ton	<p>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.</p> <p>Standardwert: Deaktiviert</p> <hr/> <p>Anmerkung: Wenn Sie den Cloud-Service Unify Video nutzen möchten, muss der SPE-Hinweiston deaktiviert werden, um die Leitung registrieren zu können, es sei denn, es wurde ein SPE-Zertifikat in das System importiert.</p> <hr/>
SIP Prov. zu SIP Prov. transit	<p>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.</p> <p>Standardwert: Deaktiviert</p>
Wahl von * und # auf Leitungsschnittstellen	<p>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.</p> <p>Standardwert: Deaktiviert</p>

Parameter	Beschreibung
Richtungskennzahl für MEX hinzufügen	<p>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.</p> <p>Standardwert: Deaktiviert</p>
CMI MWI Hinweiston	<p>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.</p> <p>Standardwert: Deaktiviert</p>
Automatisches OpenStageTDM Telefon-Software-Update	<p>Wenn dieses Flag aktiviert ist und die Softwareversion eines TDM-Telefons älter ist als die Softwareversion des Systems, wird die Software des Telefons automatisch aktualisiert.</p> <p>Standardwert: Aktiviert</p>
Indirekte Richtungsverbindungen gemäß VBZ-Matrix einschränken	<p>Wenn sich Niederlassungen einer Firma in verschiedenen Städten befinden, dann kann jede Niederlassung eine Leitung zum lokalen (staatlichen) Telekommunikationsanbieter haben. Zusätzlich können diese Niederlassungen über private Querverbindungen untereinander verbunden sein.</p> <p>Aufgrund staatlicher Auflagen (z. B. in Indien) kann es verboten sein, die folgende Verbindung zu schalten: Ein Teilnehmer benutzt die private Querverbindung von seinem Kommunikationssystem zum privaten Kommunikationssystem in der anderen Stadt und dann eine Leitung des staatlichen Telekommunikationsanbieters, um ein lokales externes Ziel zu erreichen. Stattdessen sollte für die Verbindung zwischen den Städten auch eine direkte Leitung des staatlichen Telekommunikationsanbieters benutzt werden. Diese Anforderung wurde wie folgt realisiert:</p> <ul style="list-style-type: none"> • Verbindungen zwischen privaten Querleitungen können durch Konfigurieren der CON-Matrix eingeschränkt werden. • Für private Querleitungen, die die Funktionen Rufweiterleitung, Transfer und Konferenz beinhalten, wurde das Kennzeichen "Indirekte Trunk-Gruppenverbindungen gemäß VBZ-Matrix beschränken" eingeführt. Das Aktivieren/Deaktivieren dieses Flags hat die folgenden Auswirkungen: <ul style="list-style-type: none"> - Aktiviert: Anrufe zwischen Städten, die private Querleitungen verwenden, sind eingeschränkt. - Deaktiviert: Anrufe zwischen Städten, die private Querleitungen verwenden, sind erlaubt. <p>Standardwert: Deaktiviert</p>
Offene Nummerierung	

Parameter	Beschreibung
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	
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. Leistungsbelegung	Bei aktiviertem Flag belegen ausgehende Rufe bei fehlerhaftem Verbindungsaufbau (z.B. keine ACK-Quittung) zyklisch neue ISDN-Amtsleitungen. Leitungsnummern oder Richtungsnummern werden hochgezählt. Standardwert: Aktiviert
Einschränkung für UC-Anrufe	

Parameter	Beschreibung
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

Parameter	Beschreibung
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
Wahlende bei unvollständiger Wahl	Wird die Wahl nicht innerhalb einer bestimmten Zeit fortgesetzt, so wird automatisch ein Wahlende erzeugt. Wertebereich: 10 - 20 s
AB TIn 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

Parameter	Beschreibung
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	Dieser Timer 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
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

Parameter	Beschreibung
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 (I WV-Leitungen). Standardwert: 0 s
NSA Belegungspulszeit	Nummernschalter-Arbeitskontakt (I WV-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
I WV NoFe Minimale Zwischenwahlzeit	Zeit zwischen Wahlziffern bei I WV-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

Experten-Modus

Parameter	Beschreibung
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 Aufmerksamkeitsston bei HKZ-Transit-Verbindungen	<p>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.</p> <p>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.</p> <p>Wertebereich: 120 s - 42 min</p>
Zeit vom Aufmerksamkeitsston bis zum Auslösen...	<p>Erfolgt eine zeitliche Überwachung von Transit-Verbindungen, so erfolgt nach Ablauf des Überwachungstimers ein Aufmerksamkeitsston. Damit das Gespräch beendet werden kann, wird die Verbindung nicht sofort getrennt, sondern erst nach Ablauf dieser Zeit.</p> <p>Wertebereich: 10 - 650</p>
Auslösetimer für HKZ	<p>Ein Ruf einer HKZ-Leitung über Durchwahl (DuWa) wird nach dieser Zeit ausgelöst, wenn kein Gespräch zustande kommt.</p> <p>Wertebereich: 30 s - 254 min</p>
Nach Halten wird ein Aufmerksamkeitsston geschaltet (Italien)	<p>Nach Ablauf dieser Zeit erfolgt bei gehaltenen Verbindungen ein Anklopfen bei der haltenden Nebenstelle (ITL).</p> <p>Wertebereich: 30 - 180 s</p>
LCR: Künstliches Wahlende	<p>Wartezeit nach der letzten Ziffer bis Wahlende angenommen wird (Blockwahl LCR).</p> <p>Standardwert: 5 s</p>
Überwachung eines UCD-Rufes auf einer analogen Leitung	<p>Zeit für das Auslösen eines HKZ-Anrufes auf eine UCD-Gruppe, wenn es zu keinem Verbindungsaufbau gekommen ist.</p> <p>Wertebereich: 10 - 3810 s</p>
Überwachung eines Übergeben vor Melden an eine UCD-Gruppe (nur für Entwicklung)	<p>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.</p> <p>Wertebereich: 10 - 3810 s</p>
Verzögerungs-Timer für PC-VPL	<p>Zeit bis Update Message zum PC-Vermittlungsplatz (Business Attendant) gesendet wird.</p> <p>Wertebereich: 300 ms</p>

Parameter	Beschreibung
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
Sonderbesetztton, wenn ZieTln. 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. Falls 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

Parameter	Beschreibung
<p>Name / Algorithmus</p>	<p>Der vollständige Namen wird über drei separate Felder unterstützt: Vorname, Nachname und Anzeigename. Das Feld "Anzeigename" kann bis zu 16 Zeichen, die Felder "Name" und "Nachname" können bis zu 32 Zeichen enthalten.</p> <p>Für den Anzeigenamen kann einer der folgenden Algorithmen verwendet werden:</p> <ul style="list-style-type: none"> • <nachname>, < vorname> • <nachname>, <initiale des vornamens.\> • <vorname>, <nachname> • <initiale des vornamens>, <nachname> • <nachname> <p>Standardwert: <nachname>, < vorname></p> <hr/> <p>Wichtig: Die Option <vorname>, <nachname> wird für MULAP-Benutzer in UC Suite nicht erkannt. Wenn diese Option verwendet wird, erscheinen der Vorname und Nachname des UC Suite Benutzers zusammen im Feld Vorname im UC-Benutzerverzeichnis und das Feld Nachname bleibt leer. Verwenden Sie in diesem Fall den Standardwert der Option, wobei ein Komma als Trennzeichen verwendet wird.</p> <hr/>
<p>Übergeben vor Melden</p>	<p>Bei Übergeben vor Melden kann entweder die Rufnummer des Übergebenen oder die Rufnummer des Übergebenden beim angerufenen Teilnehmer angezeigt werden. 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.</p> <p>Standardwert: Übergeben an</p>
<p>Wiederanruf</p>	<p>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 empfängt einen Rufton, bis entweder B antwortet oder A zurückruft. Unter diesem Punkt kann konfiguriert werden, ob im Display des Übergabeziels B der Teilnehmer A (Anrufer) oder C (Übergeben-Ziel) angezeigt wird. Geht von Teilnehmer A ein Wiederanruf aus, so bekommen beide Teilnehmer „meldet sich nicht“ im Display angezeigt.</p> <p>Standardwert: Übergeben-Ziel</p>

Parameter	Beschreibung
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
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). 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
Internes 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: kein: 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

Parameter	Beschreibung
Internes Telefonbuch über Unified-Verzeichnis	Ist dieses Flag aktiviert, kann der Benutzer in allen Verzeichnissen nach Kontakten suchen. Die Suchanfragen werden als Anforderungen an das Unified-Verzeichnis verarbeitet. Wenn das Flag nicht aktiviert ist, werden die Suchanfragen lokal vom System verarbeitet. Standardwert: Aktiviert
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 Rufweitschaltung 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

Parameter	Beschreibung
SST mit Übergabeoption (für Rufnr. des Anrufers)	<p>Wenn das Flag aktiviert ist und der Benutzer (während eines aktiven Anrufs) die Menüoption "Übertragung starten?" wählt, wird die Übertragung als Einzelschritt-Übergabe ausgeführt (kein Rückfragegespräch). Entscheidet sich der Benutzer, zuerst eine Rückfrage durchzuführen (z. B. Option „Enquiry?“) und danach den neuen Anruf an den gehaltenen Teilnehmer weiterzuleiten, erfolgt die Übertragung als normale Übergabe ohne Rückfrage. Bei einer Einzelschritt-Übergabe wird die rufende Nummer beim Klingeln des Mobilgeräts am externen Ziel angezeigt, d. h., der angerufene Teilnehmer sieht die rufende Nummer und nicht die Nummer des übergebenden Teilnehmers, wenn der Anruf von einem Systemgerät übergeben wird. Das Flag "Rufnummer transparent weiterreichen" muss ebenfalls aktiviert sein.</p> <p>Standardwert: Deaktiviert</p> <hr/> <p>Anmerkung: Wenn der übergebene Teilnehmer ein externes Gerät ist, muss die Funktion "CLIP no screening" (Teilnehmerrufnummer unterdrücken) vom Netzanbieter unterstützt werden und aktiviert sein. Andernfalls wird aus dem Amt die Standard-Durchwahl des Systems verwendet, oder der Anruf wird vom Amt abgelehnt.</p> <hr/>

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 Timeout
DISA intern	
Rufnummer	DISA Intern bezieht sich auf die Nutzung an einem anderen, mittels IP-vernetzten Knoten.
Mobility Callback	

Parameter	Beschreibung
Durchwahl	Die Authentifizierung mittels Passwort entfällt, wenn ein als Mobility-Rufnummer erkannter Anruf von extern auf die Mobility Callback-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/Attendant/Hotline

Parameterbeschreibung der Registerkarten:

- **Abwurf/VPL/Hotline ändern**

Parameter	Beschreibung
Abwurfplatz	
Tag/Nacht	Rufnummer des Abwurfplatzes. Der Abwurfplatz kann für die 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 Rufwefterschaltung festgelegten Anzahl von Ruftönen der Abwurfplatz gerufen. Aus einem Sammelanschluss erfolgt kein Abwurf. Der Ruf wird wieder zum ersten Sammelanschluss-Teilnehmer weitergeschaltet und verbleibt im Sammelanschluss. Standardwert: Aktiviert
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: Deaktiviert

Experten-Modus

Parameter	Beschreibung
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: Deaktiviert
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: Aktiviert
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	
Interne Rufnummer	Über diese Rufnummer kann der Abwurfplatz von internen Geräten aus erreicht werden. 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	
Wart. 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 Rufweitschaltung zu einem konfigurierbaren Überlaufziel. Wertebereich: 1-15
Wartezeit	Hier kann eine Wartezeit in Sekunden eingegeben werden. Nach Überschreitung dieser Zeit erfolgt eine Rufweitschaltung 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: Deaktiviert
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: Deaktiviert
Sonstige Kriterien	
Anklopfen im Besetzfall	Ist dieses Flag aktiviert, ist bei sämtlichen Teilnehmern im Kommunikationssystem das Leistungsmerkmal "Anklopfen" aktiv ist. Standardwert: Aktiviert

Parameter	Beschreibung
Sonstiges Anklopfen durch VPL	<p>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 Anklopfeschutzes (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 Anklopfeschutz 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.</p> <p>Standardwert: Deaktiviert</p>
Aufschalten durch VPL	<p>Ist dieses Flag aktiviert, ist der Abwurfplatz für das Leistungsmerkmal "Aufschalten" berechtigt. Damit kann er sich in ein Gespräch eines internen Teilnehmers einschalten.</p> <p>Standardwert: Aktiviert</p>

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	<p>Unter Windows Server ADS ist ein Anonymus-Zugriff nicht möglich. In diesem Fall hier Benutzernamen und Kennwort für die LDAP-Anbindung eingeben.</p> <p>Wertebereich: max. 48 Zeichen.</p>
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

Parameter	Beschreibung
Suchanfrage	Muster für die Suchanfrage an den LDAP-Server. Als Platzhalter für den zu suchenden Namen muss das Zeichen \$ eingegeben werden. Beachten Sie, dass ein Suchmuster nicht mit einem regulären Ausdruck beginnen kann. 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, Ö, Ø, Ù, 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
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

Anmerkung: Damit die LDAP-Ressourcen angezeigt werden können, müssen Sie im Menü **Display** unter **Grundeinstellungen > Display > Internes Telefonbuch** die entsprechende Option auswählen. Für weitere Informationen siehe Kapitel [28.3.1.3 Grundeinstellungen > System > Display](#).

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. Jede dieser Standard-Meldungen 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-Datei im UTF-8-Format importiert werden. Bereits bestehende Kurzwahlnummern werden vor dem Import gelöscht. Eine XML-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. Anmerkung: Der Import von Kurzwahllisten aus CSV-Dateien wird nicht mehr empfohlen und nur noch bei Bestandskunden unterstützt.

27.3.1.10 Grundeinstellungen > System > Service Codes

Leistungsmerkmale können über das Telefon mittels Servicekennzahlen aktiviert und deaktiviert werden. Servicecodes werden bei einem Circuit Anruf nicht unterstützt. Die Standard-Servicekennzahlen können geändert werden, wobei zu beachten ist, dass die Vergabe der Kennzahlen konsistent ist.

Zusätzlich können die beiden Kennzahlen geändert werden, die bei IWW-Telefonen und ISDN-Endgeräten den * (Stern, Standard: 75) und die # (Raute, Standard: 76) ersetzen (Substitutionen).

27.3.1.11 Grundeinstellungen > System > HFA-Registrierungs-Passwort

Parameterbeschreibung der Registerkarten:

- **HFA-Registrierungs-Passwort**

Parameter	Beschreibung
	Voraussetzung für die Wirksamkeit dieser Parameter ist, dass die Systemtelefone den DLI des Systems nutzen und dieser die Systemtelefone mit den erforderlichen Parametern versorgen kann.
	HFA-Registrierungs-Passwort ändern Das HFA-Registrierungs-Passwort kann vom Administrator geändert werden
Authentifizierung für HFA-Geräte durchsetzen	<p>In der Aufklappliste stehen die folgenden Optionen zur Verfügung:</p> <ul style="list-style-type: none"> • Nein (Standardwert): Es wird keine Authentifizierung angewendet <hr/> <p>Anmerkung: Wenn diese Option ausgewählt ist, sind die Passwortfelder deaktiviert. Durch Klicken auf die Schaltfläche Übernehmen wird die Authentifizierung für alle HFA-Geräte deaktiviert.</p> <hr/> <ul style="list-style-type: none"> • Nur Geräte mit DLI: Das Passwort wird nur für Geräte übernommen, die in der DLI-Datenbank vorhanden sind und die aktiviert sind • Alle Geräte: Das Passwort wird für alle aktivieren Geräte übernommen. <hr/> <p>Anmerkung: Die Konfiguration wird für alle HFA-Teilnehmer durchgesetzt. Für Nicht-DLI-Geräte ist eine manuelle Konfiguration erforderlich.</p> <hr/>
Passwort	Das Passwort muss in dieses Feld eingegeben werden. Das Passwort muss mindestens 8 Zeichen lang sein und mindestens 1 Ziffer und/oder 1 Buchstaben enthalten.
Passwort bestätigen	Das Passwort muss in diesem Feld zu Prüfzwecken erneut eingegeben werden.

27.3.1.12 Grundeinstellungen > Gateway

Parameterbeschreibung der Registerkarten:

- **Gateway-Eigenschaften ändern**

Parameter	Beschreibung
Allgemeines	
Kunden-Name	Frei wählbarer Name des Kunden, nur für Informationszwecke (optional) Wertebereich: max. 15 Zeichen.
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 Zeichen.
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.
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.
Ortskennzahl	Angabe der Ortsnetzkenzahl, z.B. 89 für München.
Anlagenrufnummer	Angabe der Anlagenrufnummer (Kopf-Nr. ohne Tln.-Durchwahl), z.B. 7007

Experten-Modus

Parameter	Beschreibung
Vernetzungsparameter	
Knoten ID	Für jeden Knoten in einem vernetzten System muss eine eindeutige Knoten-ID vergeben werden. Damit sind die einzelnen Knoten im vernetzten System 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

27.3.1.13 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 Gateway 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.
Kennwort	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.
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.
Domänen-Name	Auswahl des DynDNS-Anbieters aus einer Liste (z.B. dyndns.org) oder manuelle Eingabe des DynDNS-Anbieters (falls Kontrollkästchen Benutzerdefinierte Domäne aktiviert ist).

Parameter	Beschreibung
Update-URL	<p>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 <i>kursiv</i> markiert) zu ergänzen.</p> <p>Beispiel einer Update-URL:</p> <pre>http://www.anydns.info/update.php? user=<username>&password=<pass>&host=<domain>&ip=<ipaddr></pre> <p>Beispiel einer Update-URL mit Base64 verschlüsselter Authentifizierung:</p> <pre>https://<b64><username>:<pass></b64>@members.dyndns.org/nic/update? hostname=<domain>&myip=<ipaddr>&wildcard=NOCHG&mx=NOCHG& backmx=NOCHG</pre> <p><b64>...</b64> für Base64 codierte Parameter</p>
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.

27.3.1.14 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 bis 1800, Standardwert: 180

27.3.1.15 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 priorisiert (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

27.3.1.16 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.

27.3.1.17 Grundeinstellungen > Datum und Uhrzeit > Zeitzone-Einstellungen

Parameterbeschreibung der Registerkarten:

- **Zeitzone-Einstellungen ändern**

Parameter	Beschreibung
Zeitzone	Lokale Zeitzone, in welcher sich das System befindet

27.3.1.18 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: aus
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.

27.3.1.19 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.
Portnummer	Portnummer des Dienstes (konfigurierbar).
Port-Typ	Zur Information wird der Port-Typ angezeigt; Single: ein einzelner Port; Min: Untergrenze für ein Port-Bereich.

Parameter	Beschreibung
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
HFA_EXT	Steuerung von HFA-Clients (CorNet-TC Serverport) für System Device@Home. Standardwert: 4062
HFA_TLS	CorNet-TC über TLS. Standardwert: 4061
HFA_TLS_EXT	CorNet-TC via TLS für System Device@Home. Standardwert: 4063
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
SIP_EXT	Rufsignalisierung für SIP-Endgeräte und ITSP-Trunking für SIP-Gerät@Home. Standardwert: 5070
SIPS	Sichere Rufsignalisierung für SIPQ Trunking. Standardwert: 5061
SIP_TLS_SUB	Sichere Rufsignalisierung für SIP-Teilnehmer. Standardwert: 5062
SIP_TLS_SUB_EXT	Sichere Rufsignalisierung für SIP-Teilnehmer für SIP-Gerät@Home. Standardwert: 5071
VSL_MULTISITE	Multi-Site-Verbindungen. Standardwert: 8778

27.3.1.20 Grundeinstellungen > Gebühren > Gebühren Ausgabe

Parameterbeschreibung der Registerkarten:

- **Gebühren Ausgabe ändern**

Experten-Modus

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 eingehenden Anrufen wird unmittelbar nach Rufbeginn ein Verbindungsdatensatz angelegt, um 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
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

Parameter	Beschreibung
LCR-Rufnummer gehend bzw. angewählte Rufnummer kommend	<p>Ist dieses Flag aktiviert, wird der Gebührendatensatz um ein zusätzliches Rufnummernfeld erweitert. Er beinhaltet:</p> <ul style="list-style-type: none"> • bei gehendem Ruf die LCR-Rufnummer, die ggf. nach Umwandlung durch LCR tatsächlich ins Amt gesendet wurde, bzw. • bei kommendem Ruf die interne Rufnummer des Wunschteilnehmers, d.h. des ersten angewählten Teilnehmers. <p>Es wird auch dann ein Gebührendatensatz ausgegeben, wenn ein Anruf auf einen besetzten Teilnehmer erfolgt. Dieser Verbindungsdatensatz entspricht in seinem Format dem Datensatz eines freien Teilnehmers mit dem Unterschied, dass die Ruf-/Gesprächsdauer auf „0“ gesetzt ist.</p> <p>Standardwert: Deaktiviert</p>
Gesprächsdatenerfassung zentral (GEZ)	
Ausgabe: keine	Keine Übertragung von Verbindungsdaten Standardwert: HTTP
Ausgabe: HTTPS	Übertragung von Verbindungsdaten an mitgelieferten Gebührenmanager oder andere Accounting-SW Standardwert: HTTP
Ausgabe: LAN-TCP-Client	Übertragung von Verbindungsdaten an externen Server via TCP/IP Standardwert: HTTP
TCP-Client	Festlegen von IP-Adresse und Portnummer eines externen Gebührenservers. Bei anfallenden Gebühren initiiert das Kommunikationssystem eine TCP/IP-Verbindung zum externen Gebührenservers. Nach dem Verbindungsaufbau werden die Gebührendaten übertragen. Die Verbindung bleibt permanent bestehen, weitere anfallende Gebühren werden übertragen, wobei jeder Datensatz separat verschickt wird.

27.3.1.21 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

Experten-Modus

Parameter	Beschreibung
Multiplikator	Dieser Multiplikator wird verwendet zur Umrechnung von Tarifeinheiten in Währungsbeträge. Wertebereich: 0 bis 65534, Standardwert: 6
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.

27.3.1.22 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: Listen-Prüfung	Eingegebene PKZ werden an Hand der PKZ-Listen auf Gültigkeit geprüft.
Prüfverfahren: Prüfung der Stellenzahl	Eingegebene PKZ werden auf ihre Stellenanzahl geprüft.
Anzahl der zu prüfenden Stellen	Gültige Stellenanzahl für PKZ. Wertebereich: 1 bis 11, Standardwert: 5
PKZ-Listen	
Liste	Für Listenprüfung können maximal 1000 PKZ eingegeben werden.
Projektkennzahl	Wertebereich: max. 11 Ziffern

27.3.1.23 Grundeinstellungen > Wiedergabegerät für Sprachnachrichten/Ansagen

Parameterbeschreibung der Registerkarten:

- **Wiedergabegerät für Sprachnachrichten/Ansagen ändern**

Parameter	Beschreibung
Sprachnachricht	
Präfix	Rufnummer der Sprachbox.
Wiedergabegerät für Ansagen	
Rufnummer	Rufnummer des Wiedergabegeräts (Announcement Player).

27.3.1.24 Grundeinstellungen > Telefonparameter-Bereitstellung

Parameterbeschreibung der Registerkarten:

- **Telefonparameter-Bereitstellung bearbeiten**

Parameter	Beschreibung
Telefonparameter-Bereitstellung	
<p>Voraussetzung für die Wirksamkeit dieser Parameter ist, dass die Systemtelefone den DLI des Systems nutzen und dieser die Systemtelefone mit den erforderlichen Parametern 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.</p> <p>Die einzelnen 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.</p>	
Telefonparameter-Bereitstellung aktivieren	Ist dieses Flag aktiviert, sind die nachfolgenden Optionen zur Bearbeitung aktiviert.
SW an @Home-Geräte verteilen	Wenn dieses Flag aktiviert ist, werden Berechtigungen für die Softwareaktualisierung über DLI für HFA@Home-Geräte erteilt.
Telefonparameter	
Die folgenden Telefoneinstellungen können hier geändert werden.	
PC Port	<p>Ist dieses Flag aktiviert, wird der PC Ethernet Port aller aktiven Systemtelefone eingeschaltet.</p> <p>Standard: deaktiviert</p>
Codec-Einstellung ist "geringe Bandbreite bevorzugt"	<p>Ist dieses Flag aktiviert, gilt für alle Systemtelefone die folgende Codec-Priorisierung: G.729 - G.711 - G.722</p> <p>Ist dieses Flag deaktiviert, gilt die folgende Codec-Priorisierung: G.722 - G.711 - G.729</p> <hr/> <p>Anmerkung: CP100 unterstützt G.722 nicht</p> <hr/> <p>Standard: deaktiviert</p>
Bilder für Anrufer anzeigen	<p>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.</p> <p>Standard: deaktiviert</p>
Telefonparametereinstellungen anwenden	
Telefonparametereinstellungen auf alle Telefone anwenden	<p>Wenn Sie dieses Flag aktivieren, werden alle lokal verwalteten Einstellungen überschrieben.</p> <p>Standard: deaktiviert</p>

Parameterbeschreibung der Registerkarten:

- **Endgeräte Info**

Folgende Informationen für jedes Gerät werden hier erwähnt:

Rufnummer, Anzeige, Gerätetyp, IP-Adresse, MAC-Adresse, Aktuelle SW-Version, HW-Version, PC-Port, Codec-Einstellung.

Parameterbeschreibung der Registerkarten:

- **Administrator-Kennwort ändern**

Der Administrator kann das Passwort für den Zugriff auf das WBM des Telefons konfigurieren.

Parameter	Beschreibung
Voraussetzung für die Wirksamkeit dieser Parameter ist, dass die Systemtelefone den DLI des Systems nutzen und dieser die Systemtelefone mit den erforderlichen Parametern versorgen kann.	
Administrator-Kennwort ändern	
Das Standard-Passwort kann vom Administrator zentral für alle über DLI verbundenen Geräte geändert werden.	
Kennwort	Das Passwort muss in dieses Feld eingegeben werden. Das Passwort muss mindestens 6 Zeichen lang sein.
Kennwort bestätigen	Das Passwort muss in diesem Feld zu Prüfzwecken erneut eingegeben werden.

Parameterbeschreibung der Registerkarten:

- **Kanonische Wahleinstellungen**

Der Administrator kann die kanonischen Wahleinstellungen an alle Desk Phone CP-HFA-Geräte massenverteilen, die DLI konfiguriert haben.

Parameter	Beschreibung
Kanonische Wahleinstellungen	
Landeskennzahl	Erforderlich - Interne Kennzahl für den Telefonstandort. Wenn sie nicht eingestellt ist, findet keine Konvertierung statt. Maximale Länge 5 Zeichen.
Nationale Vorwahlziffer	Benötigt - Vorwahlziffer der Leitung für PSTN-Wahl innerhalb des Landes. Maximale Länge 5 Zeichen.
Ortskennzahl	Benötigt - PSTN-Ortsnetzkenzahl für den Standort des Telefons. Maximale Länge 6 Zeichen.
Minimale Länge der lokalen Nummer	Benötigt - PSTN-Ortsnetzlänge der Nummern. Maximale Länge 2 Zeichen.
Lokaler Unternehmensknoten	Optional - Vorwahl des lokalen Unternehmensnetzes für ein Telefon als Nebenstelle. Maximale Länge 10 Zeichen.
PSTN-Kennzahl	Optional - Liste der Ziffern für den PSTN-Zugang. Maximale Länge 10 Zeichen.
Internationale Kennzahl	Benötigt - Liste der PSTN-Kennzahlen für das internationale Gateway. Maximale Länge 5 Zeichen.

Experten-Modus

Parameter	Beschreibung
Betreiberkennzahl	Optional - Liste der Rufnummern für die Betreiber. Maximale Länge 50 Zeichen.
Notrufnummern	Optional - Liste der Nummern, die für Notrufe verwendet werden. Maximale Länge 50 Zeichen.
Initiale Durchwahlziffern / Initiale Ziffern	Optional - Liste der Anfangsziffern für die Nebenstelle im lokalen Unternehmensnetz (definiert durch den lokalen Unternehmensknoten). Maximale Länge 50 Zeichen.
Erwarte Wählnummer	Optional - Boolescher Wert, der angibt, wann eine PSTN-Kennzahl + nationale Vorwahlziffer beibehalten und nicht in die internationale Kennzahl umgewandelt wird. Wahr/Falsch mit dem Standardwert falsch.
Kanonisches Zifferblatt	
Internrufnummern	Internrufnummern - ganzzahlig
Externe Rufnummern	Externe Rufnummern - ganzzahlig
Externe Kennzahl	Externe Kennzahl - ganzzahlig
Internationale Gateway-Kennzahl	Internationale Gateway-Kennzahl - ganzzahlig
Kanonische Wählhilfe	
Lokale Kennzahl 1-5	Optional - eine lokale Knotenkennzahl im Unternehmensnetz. Maximale Länge 10 Zeichen.
Internationale Kennzahl 1-5	Optional - die internationale Kennzahl, die der lokalen Kennzahl entspricht. Maximale Länge 30 Zeichen.

27.3.1.25 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.

Parameter	Beschreibung
Ende des LowPowerModes	Endzeitpunkt des Energiesparzustand.
IP Bandbreite wird auf 100MBit/s FDX reduziert	Anzeige der Datenrate im Energiesparzustand.

27.3.1.26 Grundinstallation > Massendaten

- Parameterbeschreibung der Registerkarten:

Parameter	Beschreibung
Port	Portnummer. Nicht editierbares Feld.
Gültigkeit	Es gibt zwei Arten der Validierung: den Front-End-Konsistenz Check und den Back-End-Konsistenz Check: a. Der Front-End-Konsistenz Check validiert Daten aus den Feldern im Fenster für den Assistenten "Massendaten" validiert, indem sie auf Inkonsistenzen und Konflikte geprüft werden. Eine rote Anzeige erscheint im Feld "Gültigkeit" unter den jeweiligen Nummern. Wenn Sie mit der Maus auf ein Popup-Fenster zeigen, erhalten Sie genaue Angaben zum Konflikt. b. Beim Back-End-Konsistenz Check werden die Daten aus den Feldern im Fenster für den Assistenten "Massendaten" validiert, indem die Daten mit den vorhandenen aber nicht anzeigbaren Daten im System verglichen werden. Dazu gehören Gruppen, MULAP, Voicemail, nationaler und internationaler Zugriff, VSL-Nummern, Richtungskennzahlen und Leitungskennzahlen (z. B. Amtszugang).
Rufnr.	Interne Rufnummer des Teilnehmers.
Durchwahl	Durchwahlnummer des Teilnehmers.
Dual-Mode-Nr.	Mobile Rufnummer des Teilnehmers.
UC Mobilnr.	Persönliche Mobiltelefonnummer des Benutzers von UC Smart oder UC Suite. Die Nummer ist im kanonischen Format, z. B.: +49 89 7007 100. Diese Nummer wird in der Ansicht Eigene persönliche Daten des Benutzers im Benutzerverzeichnis angezeigt.
E-Mail-Adresse	E-Mail-Adresse des Teilnehmers.
Anzeige	Frei wählbarer Name des Teilnehmers. Wird je nach dem für den Anzeigenamen verwendeten Algorithmus standardmäßig mit Vorname und Nachname erstellt.
Vorname	Frei wählbarer Vorname des Teilnehmers.
Nachname	Frei wählbarer Nachname des Teilnehmers.
Gerätetyp	Der dem Benutzer zugeordnete Gerätetyp. Nicht editierbares Feld.
Typ	Typ des Teilnehmers.
Typ: Frei	Der Rufnummer ist (noch) kein Teilnehmer zugeordnet.

Parameter	Beschreibung
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: 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).
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 externe Faxnachrichten vom Teilnehmer empfangen werden können.
Zugang	Anzeige der physikalischen Schnittstelle, an der das Endgerät angeschlossen ist.
Clip/Lin	Ziffernfolge, die beim einem gehenden externen Anruf beim Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird (z. B. für Notrufdienst E911 USA)
Status	Zeigt den Status des Geräts an. Aktiv oder inaktiv.

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	<p>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 durch die Application Firewall auf bestimmte IP-Adressen oder IP-Adressbereiche beschränkt oder gesperrt werden:</p> <p>Dienst / Ports</p> <p>HTTPS / 443</p> <p>Postgres / 5432</p> <p>LDAP / 389</p> <p>Manager E / 7000</p> <p>ssh (im Default gesperrt) / 22</p> <p>FTP / 21, 40000 - 40040</p> <p>Nur die gelisteten Dienste können über ein Auswahlménü 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.</p>
Regelname	Vergebener Name für die Regel
Regel aktiviert	Die Regel ist aktiviert.
Untergrenze des Quell-IP-Adressbereichs	Die untere Grenze der blockierten IP-Adressen.
Obergrenze des Quell-IP-Adressbereichs	Die obere Grenze der blockierten IP-Adressen.

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 > DHCP-Server > Globale Einstellungen eingerichtet.

Parameterbeschreibung der Registerkarten:

- **DLSC-Grundeinstellung**
- **DLSC kontaktieren**
- **DLSC Bootstrapping zurücksetzen**

Parameter	Beschreibung
Status	
Sichere Kommunikation mit dem DLS-Client	Anzeige ob (und wieviel) eine sichere Kommunikation mit dem DLS-Client aktiviert bzw. deaktiviert (0) ist

Parameter	Beschreibung
DLS-Client	
Zeitintervall 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)	Anzeige der festgelegten Seriennummer im Hexadezimalformat.
Signatur-Algorithmus-Typ	Anzeige des verwendenden Signaturalgorithmus Wertebereich: 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

Parameter	Beschreibung
Ausgestellt durch CA	Die Zertifizierungsstelle, die das Zertifikat signiert hat
Land (C)	Zweistellige Länderkennzahl
Organisation (O)	Der vollständige rechtliche Firmenname
Organisationseinheit (OU)	Die Organisationseinheit ist jener Zweig des Unternehmens, der das Zertifikat anfordert.
Allgemeiner Name (CN)	Vollständig qualifizierter Domänenname (FQDN)
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)	Zweistellige Länderkennzahl
Organisation (O)	Der vollständige rechtliche Firmenname
Organisationseinheit (OU)	Die Organisationseinheit ist jener Zweig des Unternehmens, der das Zertifikat anfordert.
Allgemeiner Name (CN)	Vollständig qualifizierter Domänenname (FQDN)
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	Öffentliche Schlüsseldaten des für die Verschlüsselung verwendeten Zertifikats
Länge des öffentl. Schlüssels	Wertebereich: 1024, 1536, 2048
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.

Experten-Modus

Parameter	Beschreibung
Seriennummer des Zertifikats	Anzeige der festgelegten Seriennummer.
Seriennummer des Zertifikats (hex)	Anzeige der festgelegten Seriennummer im Hexadezimalformat.
Signatur-Algorithmus-Typ	Anzeige des verwendenden Signaturalgorithmus. Wertebereich: 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	Die Zertifizierungsstelle, die das Zertifikat signiert hat
Land (C)	Zweistellige Länderkennzahl
Organisation (O)	Der vollständige rechtliche Firmenname
Organisationseinheit (OU)	Die Organisationseinheit ist jener Zweig des Unternehmens, der das Zertifikat anfordert.
Allgemeiner Name (CN)	Vollständig qualifizierter Domänenname (FQDN)
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)	Zweistellige Länderkennzahl
Organisation (O)	Der vollständige rechtliche Firmenname
Organisationseinheit (OU)	Die Organisationseinheit ist jener Zweig des Unternehmens, der das Zertifikat anfordert.
Allgemeiner Name (CN)	Vollständig qualifizierter Domänenname (FQDN)
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	Öffentliche Schlüsseldaten des für die Verschlüsselung verwendeten Zertifikats
Länge des öffentl. Schlüssels	Wertebereich: 1024, 1536, 2048

Parameter	Beschreibung
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 Standard: 1024
Zertifikatüberprüfung	Schaltet die Zertifikatsprüfung komplett ein oder aus. Ein Abschalten der Zertifikatsprüfung wird nicht empfohlen. Standard: Ein
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 Standard: deaktiviert
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
Sichere Neuerhandlung erzwingen (RFC 5746)	Dieses Verfahren verbessert die Sicherheit bei der Neuerhandlung der Verschlüsselungsparameter von TLS-Verbindungen. Es kann nur eingesetzt werden, wenn es auf allen verbundenen Servern ebenfalls unterstützt wird. (OpenScape Business, OpenScape 4000 und OpenScape Voice unterstützen dieses verbesserte Verfahren, HiPath 3000 unterstützt es nicht). Standard: deaktiviert

Parameter	Beschreibung
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 Standard: 24

27.3.2.6 Sicherheit > Signaling- und Payload-Encryption > SPE-Zertifikat

Parameterbeschreibung der Registerkarte:

- **SPE Zertifikat und privaten Schlüssel importieren (Datei PKCS#12)**

Parameter	Beschreibung
Entschlüsselungspasswort	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:

- **Vertrauenswürdige 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. Idap://)	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**
- **Ipssec ein-/ausschalten**

Parameter	Beschreibung
Verschlüsselungsalgorithmen	Verwendete Verschlüsselungsalgorithmen Wertebereich: AES, 3DES
Hash-Algorithmen	Standardisierte kryptologische Hashfunktion zur Berechnung eines eindeutigen 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!
Ipssec 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: sha25RSA, sha512RSA
Länge des öffentl. Schlüssels	Auswahl einer für dieses Zertifikat verwendeten Schlüssellänge Wertebereich: 2048

Parameter	Beschreibung
Beginn der Zertifikatsgültigkeit (GMT)	Zeitpunkt, ab dem das Zertifikat gültig sein soll. Die Zeitangabe wird als Greenwich Mean Time (GMT) interpretiert.
Ende der Zertifikatsgültigkeit (GMT)	Zeitpunkt, bis zu dem 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. Bei Auswahl eines anderen Formats können mehrere SAN-Einträge konfiguriert werden.
Format des DN-Namens	Dies wird normalerweise auch als Common Name RDN im Betreff des Hauptzertifikats angegeben.
Anderes Format	Andere Namen, als Allgemeiner Name angegeben
Erweiterung Alternativer Antragstellername	Wertebereich: DNS-Name, IP-Adresse, E-Mail-Adresse, Uniform resource Indicator, Andere
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. Bei Auswahl eines anderen Formats können mehrere SAN-Einträge konfiguriert werden.
CRL-Verteilungspunkt-Typ	Wertebereich: DNS-Name, IP-Adresse, E-Mail-Adresse, Uniform resource Indicator, Andere
CRL-Verteilerpunkt	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.

Parameter	Beschreibung
Entschlüsselungspasswort	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 (X.509)**

Parameter	Beschreibung
Zertifikatstyp	Dient dem sicheren Erstkontakt zwischen dem Kommunikationssystem und dem DLS
Seriennummer des Zertifikats	Anzeige der festgelegten Seriennummer.
Seriennummer des Zertifikats (hex)	Anzeige der festgelegten Seriennummer im Hexadezimalformat.
Signatur-Algorithmus-Typ	Anzeige des verwendenden Signaturalgorithmus Wertebereich: 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	Die Zertifizierungsstelle, die das Zertifikat signiert hat
Land (C)	Zweistellige Länderkennzahl
Organisation (O)	Der vollständige rechtliche Firmenname
Organisationseinheit (OU)	Die Organisationseinheit ist jener Zweig des Unternehmens, der das Zertifikat anfordert.
Allgemeiner Name (CN)	Vollständig qualifizierter Domänenname (FQDN)

Experten-Modus

Parameter	Beschreibung
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)	Zweistellige Länderkennzahl
Organisation (O)	Der vollständige rechtliche Firmenname
Organisationseinheit (OU)	Die Organisationseinheit ist jener Zweig des Unternehmens, der das Zertifikat anfordert.
Allgemeiner Name (CN)	Vollständig qualifizierter Domänenname (FQDN)
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	Öffentliche Schlüsseldaten des für die Verschlüsselung verwendeten Zertifikats
Länge des öffentl. Schlüssels	Wertebereich: 1024, 1536, 2048
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 (X.509)**

Parameter	Beschreibung
Name des Zertifikats	Eingabe des Namens, den das Zertifikat haben soll.
Datei mit dem Zertifikat	Pfad und Dateiname des Zertifikats. Beim Klicken auf "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: sha25RSA, sha512RSA
Länge des öffentl. Schlüssels	Wertebereich: 2048
Antragsteller	Daten zum Zertifikatsantragsteller gemäß den Konventionen des Standards X.509 (z.B. im Feld Land (C) DE für Deutschland).
Land (C)	Zweistellige Länderkennzahl
Organisation (O)	Der vollständige rechtliche Firmenname
Organisationseinheit (OU)	Die Organisationseinheit ist jener Zweig des Unternehmens, der das Zertifikat anfordert.
Allgemeiner Name (CN)	Vollständig qualifizierter Domänenname (FQDN)
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. Bei Auswahl eines anderen Formats können mehrere SAN-Einträge konfiguriert werden.
Format des DN-Namens	Dies wird normalerweise auch als Common Name RDN im Betreff des Hauptzertifikats angegeben.
Land (C)	Zweistellige Länderkennzahl
Organisation (O)	Der vollständige rechtliche Firmenname
Organisationseinheit (OU)	Die Organisationseinheit ist jener Zweig des Unternehmens, der das Zertifikat anfordert.
Allgemeiner Name (CN)	Vollständig qualifizierter Domänenname (FQDN)
Anderes Format	Andere Namen, als Allgemeiner Name angegeben
Erweiterung Alternativer Antragstellername	Wertebereich: DNS-Name, IP-Adresse, E-Mail-Adresse, Uniform resource Indicator, Andere

Parameter	Beschreibung
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	Eingabe des Namens, den das Zertifikat haben soll.
Entschlüsselungspasswort	Passwort zur Entschlüsselung des Peer-Zertifikats Wertebereich: min. 7 und max. 32 Zeichen
Datei mit dem Zertifikat	Klicken Sie auf Durchsuchen. Ein Suchdialog wird angezeigt.
Fingerabdruck des Zertifikats anzeigen	Klicken Sie auf diese Schaltfläche, um die Integrität des Zertifikats zu überprüfen.
Zertifikat aus Datei importieren	Klicken Sie auf diese Schaltfläche, um ein Zertifikat zu 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. unbekanntem Port.
Ziel-Port	Anzeige der Ziel-Port-Nummer. Wird als Port die "0" angezeigt, so entspricht das einem beliebigen bzw. unbekanntem 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. unbekanntem 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. unbekanntem 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. unbekanntem 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. unbekanntem 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.

Experten-Modus

Parameter	Beschreibung
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 Senderegeln	Einrichtung der Senderegeln unter VPN>Regeln
Zugehörige Regeln: Zugehörige Empfangsregeln	Einrichtung der Empfangsregeln unter VPN>Regeln
Tunneln	
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).
Regel	
Zielstelle	Statusanzeige im Ziel. Wertebereich: Senden/Empfangen

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	Zeigt an, wie die IP-Pakete durch diese Regel behandelt werden: "pass" bedeutet, dass die IP-Pakete weitergeleitet werden; "deny" bedeutet, dass sie nicht weitergeleitet werden.
Verschlüsselung erforderlich	Anzeige einer Verschlüsselung für diese Regel. Das Verschlüsselungsverfahren wird über den zugeordneten Tunnel definiert.
Regel-Status	Statusanzeige in der Regel. Wertebereich: Aktiviert / Deaktiviert
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.	
Type	Anzeige des Typs für die Quelladresse und die Zieladresse (möglich sind: Host, Subnetz, IP Adressbereich und DNS-Name).
Adresse (unterste des Bereiches)	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	Dies wird festgelegt, falls für die Übertragung ein Bereich von Quell-/Zieladressen erforderlich ist.
Zieladresse	
Type	Anzeige des Typs für die Quelladresse und die Zieladresse (möglich sind: Host, Subnetz, IP Adressbereich und DNS-Name).

Parameter	Beschreibung
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	Dies wird festgelegt, falls für die Übertragung ein Bereich von Quell-/Zieladressen erforderlich ist.
Dienstdaten	
Anzeige des Dienstes, auf den die Verschlüsselung beschränkt wird. Soll die Verschlüsselung nicht auf einen Dienst beschränkt sein, wählen Sie "Beliebiger Dienst" aus.	
Name des Dienstes	Eingabefeld für den Namen des zu konfigurierten 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	Wählen Sie die für die Übertragung verwendete IP-Protokoll aus Wertebereich: ICMP, TCP, UDP

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

Parameter	Beschreibung
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 Senderegeln	Einrichtung der Senderegeln unter VPN>Regeln
Zugehörige Regeln: Zugehörige Empfangsregeln	Einrichtung der Empfangsregeln unter VPN>Regeln
Tunneln	
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	

Experten-Modus

Parameter	Beschreibung
Zielstelle	Statusanzeige im Ziel. Wertebereich: Senden/Empfangen
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	Zeigt an, wie die IP-Pakete durch diese Regel behandelt werden: "pass" bedeutet, dass die IP-Pakete weitergeleitet werden; "deny" bedeutet, dass sie nicht weitergeleitet werden.
Verschlüsselung erforderlich	Anzeige einer Verschlüsselung für diese Regel. Das Verschlüsselungsverfahren wird über den zugeordneten Tunnel definiert.
Regel-Status	Statusanzeige in der Regel. Wertebereich: Aktiviert / Deaktiviert
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.	
Type	Anzeige des Typs für die Quelladresse und die Zieladresse (möglich sind: Host, Subnetz, IP Adressbereich und DNS-Name).
Adresse (unterste des Bereiches)	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	Dies wird festgelegt, falls für die Übertragung ein Bereich von Quell-/Zieladressen erforderlich ist.
Zieladresse	
Type	Anzeige des Typs für die Quelladresse und die Zieladresse (möglich sind: Host, Subnetz, IP Adressbereich und DNS-Name).

Parameter	Beschreibung
Adresse (unterste des Bereiches)	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	Dies wird festgelegt, falls für die Übertragung ein Bereich von Quell-/Zieladressen erforderlich ist.
Dienstdaten	
Anzeige des Dienstes, auf den die Verschlüsselung beschränkt wird. Soll die Verschlüsselung nicht auf einen Dienst beschränkt sein, wählen Sie "Beliebiger Dienst" aus.	
Name des Dienstes	Eingabefeld für den Namen des zu konfigurierten 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	Für die Übertragung zu verwendende IP-Protokoll Wertebereich: ICMP, TCP, UDP
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).

Parameter	Beschreibung
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
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

Anmerkung: 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.
Service	Anzeige des Dienstes, auf den die Verschlüsselung beschränkt wird. Ist die Verschlüsselung nicht auf einen Dienst beschränkt, so wird "Beliebiger Dienst" angezeigt.
Aktion für die Regel	Zeigt an, wie die IP-Pakete durch diese Regel behandelt werden: "pass" bedeutet, dass die IP-Pakete weitergeleitet werden; "deny" bedeutet, dass sie nicht weitergeleitet werden.
Verschlüsselung erforderlich	Anzeige der Verschlüsselung. Das Verschlüsselungsverfahren wird über den zugeordneten Tunnel definiert.
Regel-Status	Statusanzeige in der Regel. Wertebereich: Aktivierung / Deaktivierung
Status im IP-Stack	Statusanzeige im IP-Stack. Wertebereich: Aktivierung / Deaktivierung
Quelladresse	
Type	Anzeige des Typs für die Quelladresse. Wertebereich: Host, Subnetz, IP-Adressbereich, DNS-Name
Adresse (unterste des Bereiches)	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 / obersteAdr. des Bereichs	Dies wird festgelegt, falls für die Übertragung ein Bereich von Quell-/Zieladressen erforderlich ist.
Zieladresse	

Parameter	Beschreibung
Type	Anzeige des Typs für die Zieladresse. Wertebereich: Host, Subnetz, IP-Adressbereich, DNS-Name
Adresse (oberste des Bereichs)	
Subnetzmaske / oberste Adr. des Bereichs	Dies wird festgelegt, falls für die Übertragung ein Bereich von Quell-/Zieladressen erforderlich ist.
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.
Service	Anzeige des Dienstes, auf den die Verschlüsselung beschränkt wird. Ist die Verschlüsselung nicht auf einen Dienst beschränkt, so wird "Beliebiger Dienst" angezeigt.

Parameter	Beschreibung
Aktion für die Regel	Zeigt an, wie die IP-Pakete durch diese Regel behandelt werden: "pass" bedeutet, dass die IP-Pakete weitergeleitet werden; "deny" bedeutet, dass sie nicht weitergeleitet werden.
Verschlüsselung erforderlich	Anzeige der Verschlüsselung. Das Verschlüsselungsverfahren wird über den zugeordneten Tunnel definiert.
Regel-Status	Statusanzeige in der Regel. Wertebereich: Aktiviert / Deaktiviert
Status im IP-Stack	Statusanzeige im IP-Stack. Wertebereich: Aktivierung / Deaktivierung
Quelladresse	
Type	Anzeige des Typs für die Quelladresse. Wertebereich: Host, Subnetz, IP-Adressbereich, DNS-Name
Adresse (unterste des Bereiches)	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	Dies wird festgelegt, falls für die Übertragung ein Bereich von Quell-/Zieladressen erforderlich ist.
Zieladresse	
Type	Anzeige des Typs für die Zieladresse. Wertebereich: Host, Subnetz, IP-Adressbereich, DNS-Name
Adresse (oberste des Bereichs)	
Subnetzmaske / oberste Adr. des Bereichs	Dies wird festgelegt, falls für die Übertragung ein Bereich von Quell-/Zieladressen erforderlich ist.
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 TLS 1.2-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: sha256RSA, sha512RSA
Länge des öffentl. Schlüssels	Wertebereich, Standardwert: 2048

Parameter	Beschreibung
Beginn der Zertifikatsgültigkeit (GMT)	
Zeitpunkt, ab dem das Zertifikat gültig sein soll. 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)	
Zeitpunkt, bis zu dem das Zertifikat gültig sein soll. 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 (z.B. im Feld Land (C) DE für Deutschland). Alle vier Felder müssen ausgefüllt werden.	
Land (C)	Zweistellige Länderkennzahl
Organisation (O)	Der vollständige rechtliche Firmenname
Organisationseinheit (OU)	Die Organisationseinheit ist jener Zweig des Unternehmens, der das Zertifikat anfordert.
Allgemeiner Name (CN)	Vollständig qualifizierter Domänenname (FQDN)
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. Bei Auswahl eines anderen Formats können mehrere SAN-Einträge konfiguriert werden.	
Format des DN-Namens	Dies wird normalerweise auch als Common Name RDN im Betreff des Hauptzertifikats angegeben.
Anderes Format	Andere Namen, als Allgemeiner Name angegeben
Erweiterung Alternativer Antragstellername	(optional) Wertebereich, Standardwert: DNS-Name, IP-Adresse, E-Mail-Adresse, Uniform ResourceIndicator, Andere
Alternativer Antragstellername	
CRL-Verteilungspunkt-Typ	Wertebereich: DNS-Name, IP-Adresse, E-Mail-Adresse, Uniform resource Indicator, Andere
CRL-Verteilerpunkt	Hier kann (optional mit einer URL) die Stelle angegeben werden, von der aus Zertifikatssperlisten (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.
Entschlüsselungspasswort	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: sha256RSA, sha512RSA
Länge des öffentl. Schlüssels	Wertebereich: 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)	Zweistellige Länderkennzahl
Organisation (O)	Der vollständige rechtliche Firmenname
Organisationseinheit (OU)	Die Organisationseinheit ist jener Zweig des Unternehmens, der das Zertifikat anfordert.
Allgemeiner Name (CN)	Vollständig qualifizierter Domänenname (FQDN)
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. Bei Auswahl eines anderen Formats können mehrere SAN-Einträge konfiguriert werden.	

Parameter	Beschreibung
Format des DN-Namens	Dies wird normalerweise auch als Common Name RDN im Betreff des Hauptzertifikats angegeben.
Anderes Format	Andere Namen, als Allgemeiner Name angegeben
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 .
Entschlüsselungspasswort	Passwort, 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-Zugriffsfiler**

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, 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

27.3.2.25 Sicherheit > SQL Sicherheit

Parameterbeschreibung der Registerkarte:

- **SQL-Zugangskennwort**

Parameter	Beschreibung
Neu generieren	Es wird ein verschlüsseltes SQL-Passwort erstellt, das der Benutzer nicht kennt.
Default aktivieren	Das Standard-SQL-Passwort wird aktiviert.

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: <code>commsystem</code> 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: <code>commsystem.mynet.home</code>

27.3.3.2 Netzwerkschnittstellen > Mainboard > LAN 1 (WAN)

Parameterbeschreibung der Registerkarten:

- **LAN 1-Modus anzeigen**
- **LAN 1-Schnittstelle bearbeiten**
- **ACD ändern**

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.

Parameter	Beschreibung
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.
Internetzugang über einen externen Router	Der Zugang zum Internet erfolgt über einen externen Router. Dieses Flag wird intern vom Internet-Konfigurationsassistenten verwendet und sollte nicht geändert werden.
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-Schnittstelle.
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 Vollduplex-Betrieb.
Ethernet-Link-Modus: 100HDX	100 Mbit/s, Vollduplex.
Ethernet-Link-Modus: 100FDX	100 Mbit/s, Vollduplex.
Ethernet-Link-Modus: 1000FDX	1000 Mbit/s, Vollduplex.
Netzwerkadress-Übersetzung (NAT)	NAT (Network Address 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.

Experten-Modus

Parameter	Beschreibung
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 Priorität / 7= höchste Priorität. Wertebereich, Standardwert: 0 - 7, 3
Fax/Modem-Payload	Prioritätsklasse für die Fax- und Modemdaten der IP-Verbindung. 0 = geringste Priorität / 7= höchste Priorität. Wertebereich, Standardwert: 0 - 7, 5
Netzwerksteuerung	Prioritätsklasse für die Daten der Netzwerksteuerung (z.B. Übermittlung von SNMP-Traps). 0 = geringste Priorität / 7= höchste Priorität. Wertebereich, Standardwert: 0 - 7, 0
Sprach-Payload	Prioritätsklasse für die Sprachdaten der IP-Verbindung. 0 = geringste Priorität / 7= höchste Priorität. Wertebereich, Standardwert: 0 - 7, 5
Internet-Zugangsdaten für ...	
Anschlusskennung / Benutzername / T-Online-Nummer / Mitbenutzernummer/ Suffix / Internetzugangs-Kennung / DSL-Login ...	Zugangsdaten des Internet-Service-Providers.
CHAP-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.

Parameter	Beschreibung
Lokale IP-Adresse der PPP-Verbindung	IP-Adresse, die vom ISP für den Internet-Zugang zugeteilt wurde.
IP-Address-Aushandlung	Auswahl, wie die IP-Adresse zwischen den Verbindungspartnern beim Verbindungsaufbau ausgehandelt werden soll.
IP-Adress-Aushandlung: konfigurierte IP-Adresse nutzen	Es ist nur die konfigurierte IP-Adresse möglich.
IP-Adress-Aushandlung: jede IP-Adresse akzeptieren	Es wird jede vom Partner vorgeschlagene Adresse akzeptiert.
IP-Adress-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.
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.
Remote-Subnetz-Maske für die Kontrollverbindung	Netzmaske, die vom ISP für die PPTP-Verbindung zugeteilt wurde.
Short-Hold-Modus	

Experten-Modus

Parameter	Beschreibung
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-Authentifizierungsmodus	Aktivierung und Art der PAP-Authentifizierung für die PPP-Verbindung: nicht benutzt, PAP-Client, PAP-Host.
PAP-Kennwort	Kennwort für die PAP-Authentifizierung.
CHAP-Authentifizierungsmodus	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	
Netzwerkadress-Übersetzung (NAT)	NAT (Network Adress Translation) ist eingeschaltet. Folgende Protokolle werden unterstützt: TCP, UDP und ICMP (nur im Passivmodus).
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.
Short-Hold-Zeit (s)	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

Parameter	Beschreibung
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 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.
Bandbreitensteuerung für Sprach-Verbindungen	Die Bandbreitensteuerung verhindert das Überbuchen der verfügbaren Übertragungsraten mit Sprachverbindungen innerhalb einer Multilink-Verbindung. D. h., bei aktivierter Header-Kompression sind maximal 5 Sprachverbindungen über einen B-Kanal erlaubt. 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 ändern**

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.

Experten-Modus

Parameter	Beschreibung
MAC-Adresse	Anzeige der MAC-Adresse des Kommunikationssystems.
Ethernet-Link-Modus	Modus der LAN-Schnittstelle.
Ethernet-Link-Modus: Auto	<p>Automatisches Umschalten zwischen 100 und 1000 Mbit/s Vollduplex-Betrieb. In diesem Modus kann das Power-Management aktiviert werden.</p> <p>Nach der Migration auf V2R3 oder höher muss für die gewünschte Ethernet-Verbindung über die Netzwerkschnittstellenseite oben auf "Übernehmen" gedrückt werden, damit der Wert auf "Auto" gesetzt wird.</p> <p>Anderenfalls müssen die Systeme vor der Migration auf "Auto" oder 100 gesetzt werden.</p>
Ethernet-Link-Modus: 100HDX	100 Mbit/s, Vollduplex. 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	<p>Prioritätsklasse für den Verbindungsaufbau. 0 = geringste Priorität / 7= höchste Priorität.</p> <p>Wertebereich, Standardwert: 0 - 7, 3</p>
Fax/Modem-Payload	<p>Prioritätsklasse für die Fax- und Modemdaten der IP-Verbindung. 0 = geringste Priorität / 7= höchste Priorität.</p> <p>Wertebereich, Standardwert: 0 - 7, 5</p>
Netzwerksteuerung	<p>Prioritätsklasse für die Daten der Netzwerksteuerung (z.B. Übermittlung von SNMP-Traps). 0 = geringste Priorität / 7= höchste Priorität.</p> <p>Wertebereich, Standardwert: 0 - 7, 0</p>
Sprach-Payload	<p>Prioritätsklasse für die Sprachdaten. 0 = geringste Priorität / 7= höchste Priorität.</p> <p>Wertebereich, Standardwert: 0 - 7, 5</p>

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.
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 Vollduplex-Betrieb.
Ethernet-Link-Modus: 100HDX	100 Mbit/s, Vollduplex.
Ethernet-Link-Modus: 100FDX	100 Mbit/s, Vollduplex.
Ethernet-Link-Modus: 1000FDX	1000 Mbit/s, Vollduplex.

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.

Parameter	Beschreibung
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 bestätigen	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 bestätigen	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 Subnetzmaske definiert die Größe des Subnetzes. Beispiel: 255.255.255.0.

Parameter	Beschreibung
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	
Domain-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).
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).
Dynamisch DNS aktualisieren	Ist das Kontrollkästchen aktiviert, wird ein dynamisches Update des DNS-Servers erlaubt. Standard: nicht aktiviert. <hr/> Anmerkung: Wenn die Option "Dynamische DNS-Aktualisierung" aktiviert ist, muss der Domänenname im Feld "IP-Adresspool" bzw. "Domänenname" konfiguriert werden. <hr/>

Parameter	Beschreibung
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 Subnetzmaske definiert die Größe des Subnetzes. Standardeinstellung: 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).
Gateway 3	IP-Adresse, unter der ein drittes Default Gateway (Router) zu erreichen ist (optional).

Parameter	Beschreibung
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.
Domain-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
Hostname	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	

Experten-Modus

Parameter	Beschreibung
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.
Standardgateway 1	IP-Adresse, unter der ein zweites Default Gateway (Router) zu erreichen ist (optional).
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.
Domain-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).

27.3.3.10 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 zugewiesen wurde.
Client-ID	Client-ID des IP-Teilnehmers. Ist die Client-ID nicht verfügbar, wird die MAC-Adresse des IP-Teilnehmers angezeigt.
Hostname	Name oder Rufnummer des IP-Teilnehmers, dem eine IP-Adresse zugewiesen 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 zugewiesen wurde.
Client-ID	Client-ID des IP-Teilnehmers. Ist die Client-ID nicht verfügbar, wird die MAC-Adresse des IP-Teilnehmers angezeigt.
Hostname	Name oder Rufnummer des IP-Teilnehmers, dem eine IP-Adresse zugewiesen 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 > Application Board > Host-Name

Parameterbeschreibung der Registerkarten:

- **Host-Name ändern**

Parameter	Beschreibung
Host-Name	<p>Host-Name des Application Boards - frei wählbar. Beispiel: applboard</p> <p>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</p>

27.3.3.13 Netzwerkschnittstellen > Application Board > 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 der LAN 1-Schnittstelle.
Ethernet-Link-Modus: Auto	Automatisches Umschalten zwischen 100 und 1000 Mbit/s Vollduplex-Betrieb. In diesem Modus kann das Power-Management aktiviert werden.
Ethernet-Link-Modus: 100HDX	100 Mbit/s, Vollduplex. 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.

27.3.3.14 Netzwerkschnittstellen > Application Board > 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.
Ethernet-Link-Modus	Modus die LAN 2-Schnittstelle.
Ethernet-Link-Modus: Auto	Vollduplex-Modus. In diesem Modus kann das Power-Management aktiviert werden.
Ethernet-Link-Modus: 100HDX	100 Mbit/s Vollduplex. 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	Geben Sie als ID-Nummer des VLAN einen vom Standardwert "0" abweichenden Wert ein, wenn der verwendete Switch Probleme mit dem Standardwert "0" hat.
Layer 2-QoS-Klasse	
Signalisierungsdaten	Prioritätsklasse für den Verbindungsaufbau. 0 = geringste Priorität / 7= höchste Priorität.
Fax/Modem-Payload	Prioritätsklasse für die Fax- und Modemdaten der IP-Verbindung. 0 = geringste Priorität / 7= höchste Priorität.
Netzwerksteuerung	Prioritätsklasse für die Daten der Netzwerksteuerung (z.B. Übermittlung von SNMP-Traps). 0 = geringste Priorität / 7= höchste Priorität.
Sprach-Payload	Prioritätsklasse für die Sprachdaten der IP-Verbindung. 0 = geringste Priorität / 7= höchste Priorität.

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 zur 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.

Parameter	Beschreibung
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	<p>IP-Adresse, unter der der DNS-Server erreichbar ist.</p> <p>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.</p> <p>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).</p> <p>Im Falle eines OpenScape Business S-Systems ist ein Systemneustart erforderlich, damit die Änderungen wirksam werden.</p>

27.3.4.4 Routing > IP-Routing > Application Board > 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 Routentabelle anzeigen**
- **Statische Route hinzufügen**
- **Statische Route ändern**
- **Statische Route löschen**

Parameter	Beschreibung
Route-Index	Der Route-Index wird automatisch vergeben und nur zur Information angezeigt. Er kann nicht geändert werden.
Route-Name	<p>Name oder Beschreibung der statischen Route, frei wählbar (optional)</p> <p>Wertebereich: max. 35 Zeichen.</p>

Parameter	Beschreibung
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 > Application Board > 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.

Parameter	Beschreibung
Protokoll: TCP	<p>TCP (Transmission Control Protocol)</p> <p>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.</p>
Protokoll: UDP	<p>UDP (User Datagram Protocol)</p> <p>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.</p>

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	<p>Wiederholungsversuche, die das System zum Aufbau einer Verbindung unternehmen soll.</p> <p>Wertebereich: 0 bis 255</p>
Wahlwiederholungspause (s)	<p>Pause zwischen den Wahlwiederholungen in Sekunden.</p> <p>Wertebereich: 1 - 1,000</p>
Scripting	

Parameter	Beschreibung
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 Passwort, z.B Host=ERT005, Nutzer=KJUMBERT, Passwort=123456. Die Einträge sind wie folgt: Kennung 1 für Scripting: HOST:ERT005 - Host Kennung 2 für Scripting: USER:KJUMBERT - Neues Passwort für Scripting: PASSWORT:123456.
Kennung 2 für Scripting	Zweiter Teil der Kennung für die Anmeldung bei Internet-Providern.
Neues Passwort 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: <ul style="list-style-type: none"> • 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	Einrichten der PSTN-Anbindung: (Standardauswahl: Aktiviert).
Art der PSTN-Verbindung: Nicht konfiguriert	PSTN-Partner kann vorkonfiguriert werden. Ein Verbindungsaufbau über diesen PSTN-Partner wird mit dieser Einstellung jedoch verhindert.

Parameter	Beschreibung
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.
IP-Address-Aushandlung	Aushandlung der IP-Adresse zwischen den Verbindungspartnern beim Verbindungsaufbau.
IP-Adress-Aushandlung: konfigurierte IP-Adresse nutzen	Nur die konfigurierte IP-Adresse des PSTN-Partners wird akzeptiert.
IP-Adress-Aushandlung: jede IP-Adresse akzeptieren	Keine IP-Adress-Aushandlung
IP-Adress-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).
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

Experten-Modus

Parameter	Beschreibung
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	Eine LCP-Echo-Anforderung wird gesendet. Diese Funktion dient der Prüfung, ob die Verbindung noch aktiv ist.
Short-Hold-Modus	
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 Short-Hold-Timer wird nur von ausgehenden Paketen getriggert. Wertebereich: 10 bis 9999
Short-Hold-Gebührentaktauswertung	Geben Sie an, ob der Short-Hold-Betrieb unter Berücksichtigung des Gebührentaktes optimiert werden soll. 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-Authentifizierungsmodus	Aktivierung und Art der PAP-Authentifizierung für die PPP-Verbindung: nicht benutzt, PAP-Client, PAP-Host.
PAP-Kennwort	Kennwort für die PAP-Authentifizierung.

Parameter	Beschreibung
CHAP-Authentifizierungsmodus	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.
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	
Netzwerkadress-Übersetzung (NAT)	NAT (Network Adress Translation) ist eingeschaltet. Folgende Protokolle werden unterstützt: TCP, UDP und ICMP (nur im Passivmodus).
Address-Mapping	Adress-Mapping ist aktiviert.
QoS-Parameter der Schnittstelle	
Bandbreitensteuerung für Sprach-Verbindungen	Die Bandbreitensteuerung 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.
Anrufrichtung: Gesperrt	Die Nummer ist nicht verwendbar.
Rufrichtung : kommend	Der Partner darf anrufen, aber nicht angerufen werden.
Anrufrichtung: 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.
LCR Daten zurücksetzen	
Löschen der konfigurierten LCR Daten und Initialisierung mit LCR Standard Daten	Wird dieses Optionsfeld aktiviert, werden die konfigurierten LCR-Einträge (Wahlpläne, Wegetabellen, Wahlregeln) gelöscht und durch die Standard-Einträge ersetzt.

Tipp: Bei Fehlkonfiguration im LCR besteht die Gefahr, dass gehende Verbindungen nicht oder nur eingeschränkt möglich sind.

27.3.5.2 LCR > Berechtigungen

Parameterbeschreibung der Registerkarte:

- **LCR Berechtigungen ändern**

Parameter	Beschreibung
Index	Hierarchische Indexliste
Rufnummer	Rufnummer
Name	Name des Teilnehmers
Berechtigungsgruppe	Jeder Teilnehmer wird einer LCR-Berechtigungsgruppe (Class Of Service COS) zugewiesen. Standardmäßig sind alle Teilnehmer mit maximaler LCR-Berechtigung (15) eingetragen Wertebereich: 1 bis 15

Tipp: 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
Rufnummernplan	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 bis zu 16 Wege (Routen) angelegt. Die Wahlregeltabelle legt fest, wie die vom Teilnehmer ausgesuchten Ziffern umgesetzt und vom Kommunikationssystem gewählt werden.

Parameter	Beschreibung
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 Kommunikationssystems 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)
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.
Amtsberichtigung	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.
Notruf	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

Parameter	Beschreibung
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 (Class Of Service COS) hat. Ist dies der Fall, erfolgt die Wahl gemäß der in der Wegetabelle eingetragenen Wahlregel. Wertebereich: 1 bis 16
Dedizierte Richtung	Es wird die Richtung verwendet, die dem Teilnehmer fest zugewiesen wurde (z.B. über die Zuweisung der Richtung beim Multisite Management).
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
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.

Parameter	Beschreibung
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 Erzungen oder Mehrere Standorte des Parameters Dediziertes Gateway .
Schaltflächen	
Blauer Pfeil in Spalte Wahlregel	Zeigt die Seite mit den Wahlregel -Parametern an.

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 definierbarer 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.
D (n)	Ziffernfolge wählen (1 bis 25 Ziffern). "D" darf in der Zeichenkette mehrmals vorkommen und an beliebigen Stellen stehen.

Parameter	Beschreibung
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)	P(n) darfin der Zeichenkette mehrmals vorkommen und an beliebigen Stellen stehen. P(n) darf von beliebigen anderen Parametern eingeschlossen sein. (1- bis 60-fache der systemweiten Pauseneinheit).
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.

Parameter	Beschreibung
MCL Two Stage	Bei MCL Two Stage wird mit einem Präfix der gewünschte Netzanbieter angewählt. Nach einer Synchronisationsphase wird zunächst ein ebenfalls konfigurierbarer Autorisierungscode 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 öffentlichen 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 Autorisierungscode 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 des Calling Service in der SETUP-Meldung über die folgenden 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, Ortsnetzkenzahl, 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".

27.3.5.6 LCR > Multisite

Parameterbeschreibung der Registerkarte:

- **Bereich ändern**

Parameter	Beschreibung
Ortskennzahl	Eingabe der Ortsvorwahl für einen Standort (inkl. führender Null, z.B. 069 für Frankfurt und 030 für Berlin). Es können unterschiedliche oder auch gleiche Ortsvorwahlen eingetragen werden.
Bereich	Eingabe des Namens für einen Standort (z.B. die zu den Ortsvorwahlen passenden Städte <code>Frankfurt</code> und <code>Berlin</code> oder bei gleichen Ortsvorwahlen die Abteilungsbezeichnungen <code>Service</code> und <code>Vertrieb</code>).
Dedizierte Richtung	Auswahl der Richtung bzw. der ITSP-Registrierung für diesen Standort.
Löschen	Löscht die markierten Standorteinträge.
Schaltflächen	

Parameter	Beschreibung
Speichern	Sichert die Änderungen.

Parameterbeschreibung der Registerkarte:

- **Teilnehmer/Gruppen ändern**

Parameter	Beschreibung
Bereich	Auswahl des Standorts für den Teilnehmer oder die Gruppe.
Dedizierte Richtung	Auswahl der Richtung bzw. der ITSP-Registrierung für den Teilnehmer oder die Gruppe.
Suche	Suche nach Teilnehmern und Gruppen, indem der Suchbegriff in die Suchfelder Rufnr , DuWa oder Name eingegeben und anschließend die Return-Taste gedrückt wird. Alle Teilnehmer und Gruppen werden aufgelistet, wenn alle Suchfelder leer sind und anschließend die Return-Taste gedrückt wird. Über die Auswahl Typ lassen sich alle Teilnehmer-Typen anzeigen (z.B. SIP Clients oder System Clients).

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	TCP (Transmission Control Protocol) TCP ist ein obligatorisches Transportprotokoll für SIP und kann hier nicht deaktiviert werden.
SIP über UDP	UDP (User Datagram Protocol) UDP ist das standardmäßige Transportprotokoll für SIP, das deaktiviert werden kann, wenn kein Endpunkt/Trunk/ITSP es verwendet. Es wird ausdrücklich empfohlen, das UDP aktiviert bleibt.
SIP über TLS	TLS (Transport Layer Security) TLS ist ein sicheres Transportprotokoll für SIP und kann hier nicht deaktiviert werden.
SIP-Registrierung	

Experten-Modus

Parameter	Beschreibung
Dauer der Registrierung (s)	<p>Intervall (in Sekunden) innerhalb dessen die Registrierung eines SIP-Endpunkts wiederholt werden muss. Der Intervallwert sollte nicht zu hoch eingestellt werden, weil die Registrierung dazu benötigt wird, festzustellen, ob ein Endpunkt außer Betrieb ist. (Der Registrierungszeitraum für ITSP-Trunks wird in den ITSP-Profilen konfiguriert).</p> <p>Wertebereich, Standardwert: 10 - 86400, 120</p>
RFC 3261 Timer-Werte	
Transaction Timeout (ms)	<p>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.</p> <p>Wertebereich, Standardwert: 2000 - 64000, 32000</p>
SIP-Session-Timer	
RFC 4028 verwenden	<p>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. Hier werden die Konfigurationsmöglichkeiten verwendet, um die Aktualisierung der Sitzung in der Leitungsschnittstelle zu steuern (für ITSPs siehe das dazugehörige Profil).</p>
Session-Expires (s)	<p>Definiert die Dauer einer SIP-Session. Der Standardwert ist „1800“.</p> <p>Der konfigurierte Wert wird für Trunking und ITSP-Schnittstellen verwendet.</p> <p>Wertebereich, Standardwert: 90 - 65535, 1800</p>
Minimal-SE (s)	<p>Definiert die kürzeste Dauer einer SIP-Session, die erlaubt ist.</p> <p>Der konfigurierte Wert wird für Trunking und ITSP-Schnittstellen verwendet.</p> <p>Wertebereich, Standardwert: 90 - 65535, 90</p>
DNS Einträge	
Sperrzeit für nicht erreichbare Ziele (s)	<p>Dieser Timer wird verwendet, um die Blacklist des SIP-Stack zu kontrollieren. Wenn ein durch DNS aufgelöster SIP-Server nicht reagiert, wird er für die Dauer der hier konfigurierten Zeit gesperrt. Der Standardwert ist 60 Sekunden. Falls redundante Server verwendet werden (Beispiel: DNS resultiert in mehreren Servern), wird ein höherer Wert empfohlen (z.B. 900).</p>
Provider-Anrufe	
Maximal mögliche Anrufe über Provider	<p>Hier wird die Anzahl der gleichzeitigen Gespräche über alle aktivierten Provider angezeigt. Der Wert wird entsprechend der verfügbaren Bandbreite und der ITSP-Konfiguration beim Einrichten konfiguriert.</p>

27.3.6.2 Sprachgateway > ITSP Loc-ID Einstellungen

Parameterbeschreibung der Registerkarten:

- ITSP Loc-Info hinzufügen

Die ITSP Loc-Info wird im SIP-Protokoll verwendet, um den Empfänger eines Notrufs über dessen geografischen Ursprung zu informieren. Im SIP-Protokoll wird das Format der Loc-ID-Info als RFC4119 & RFC5139 (XML-kodiertes Loc-Objekt im MIME-Text) festgelegt. Mit der ITSP Loc-ID können alle in den entsprechenden RFCs definierten Felder bestimmt werden, wohingegen in Ihrer bestimmten Bereitstellung nur eine Untermenge dieser Daten konfiguriert werden muss. (Beispiel: In der Schweiz wird nur das NAM-Feld für die Definition eines Ortes verwendet). Die für die Definition eines Ortes nötigen Daten erhalten Sie von Ihrem ITSP.

Parameter	Beschreibung
Loc-ID-Name	Der Name der Loc-ID.
Land	Das Land wird über den zweistelligen ISO-3166-Code identifiziert.
A1	Nationale Unterabteilungen (Staat, Region, Provinz, Präfektur)
A2	Landkreis, Gemeinde, Gun, Kreis
A3	Stadt, Gemeinde, Shi
A4	Stadt-Division, Bezirk, Stadtteil, Ward, Chou
A5	Nachbarschaft, Block
A6	Straße
PRD	Führende Straßenrichtung
POD	Trailing Straße Suffix
STS	Straße Suffix
HNO	Hausnummer, nur numerischer Teil
HNS	Hausnummer Suffix
LMK	Wahrzeichen oder Vanity Adresse
LOC	Zusätzliche Informationen Standort
FLR	Floor
NAM	Name (Wohnung, Geschäft oder Büroangestellter)
PC	Postleitzahl
ROOM	Raum
PLC	Art des Orts
PCN	Name der Postgemeinschaft
POBOX	Postfach
ADDCODE	Zusatzcode

Parameter	Beschreibung
SEAT	Sitz (Schreibtisch, Kabine, Workstation)
RD	Hauptstraßennetzes Name
RDSEC	Straßenabschnitt
RDBR	Zweig Straße Name
RDSUBBR	Sub-Zweig Straße Name
PRM	Straßenname pre-Modifikator
POM	Straßenname Post-Modifikator
Erweiterte Einstellungen aktivieren	Wenn aktiviert, können die erweiterten Parameterfelder konfiguriert werden.
BLD	Gebäude (Struktur)
UNIT	Einheit (Wohnung, Suite)

27.3.6.3 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 Komfortauschen.

Parameter	Beschreibung
Priorität	Den Audio-Codern 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 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. Die einstellbaren Werte sind von den Codern abhängig. Für die Vernetzung von OpenScape Business mit OpenScape Voice über SIP-Q V2: Cordless IP und OpenScape Mobile Connect unterstützen nur eine Framelänge von 20 ms für den G.711 Codec. 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. Für System mit Booster-Karte und/oder Booster-Server: Bei aktiviertem Flag wird die Fehlerkorrektur während im T.38-Protokoll durchgeführt. Ein Popup-Fenster wird angezeigt, um den Benutzer darüber zu informieren, dass ein manueller Neustart des Systems oder OCAB/Booster Servers erforderlich ist.
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

Parameter	Beschreibung
Verwendete Fehlerkorrektur für T.38-Fax (UDP)	<p>Legt fest, welche Methode zur Fehlerkorrektur eingesetzt werden soll.</p> <p>Werte: t38UDPFEC, t38UDPRedundancy</p> <p>Für System mit Booster-Karte und/oder Booster-Server: Wenn eine Option ausgewählt ist, wird ein Popup-Fenster angezeigt, um den Benutzer darüber zu informieren, dass ein manueller Neustart des Systems oder OCAB/Booster Servers erforderlich ist.</p> <p>Standardwert: t38UDPRedundancy</p>
T.30 Fax	
ECM aktivieren	<p>Für System mit Booster-Karte und/oder Booster-Server: Bei aktiviertem Flag wird die Fehlerkorrektur im T.30-Protokoll durchgeführt. Ein Popup-Fenster wird angezeigt, um den Benutzer darüber zu informieren, dass ein manueller Neustart des Systems oder OCAB/Booster Servers erforderlich ist.</p> <p>Standardwert: Aktiviert</p>
VoIP-Kompatibilitätsmodus	<p>Für System mit Booster-Karte und/oder Booster-Server: Dieses Flag sollte aktiviert werden, wenn Probleme mit der Faxübertragung in VoIP-Netzwerken auftreten. Ein Popup-Fenster wird angezeigt, um den Benutzer darüber zu informieren, dass ein manueller Neustart des Systems oder OCAB/Booster Servers erforderlich ist.</p> <p>Standardwert: Deaktiviert</p>
Sonstiges	
ClearChannel	<p>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. Der Parameter legt fest, ob die ClearChannel-Interface-Funktionalität aktiviert sein soll oder nicht.</p>
Rahmengröße	<p>In diesem Feld können Sie die Sampling-Rate bestimmen. Möglich sind 10, 20, 30, 40, 50 und 60 Millisekunden (ms).</p> <p>Wertebereich, Standardwert: 10 - 60, 20</p>
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
Übertragung von DTMF Tönen nach RFC2833	Übertragung outband (über die SIP-Signalisierung), empfohlene Betriebsweise um Töne sicher zu übertragen
Payload Type für RFC2833	<p>Anpassung ggf. abhängig vom Kommunikationspartner erforderlich</p> <p>Wertebereich, Standardwert: 96 - 126, 98</p>

Parameter	Beschreibung
Redundante Übertragung der RFC2833 Töne nach RFC2198	Dient zur Erhöhung der Übertragungssicherheit

27.3.6.4 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 Komfortauschen.
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.
Zielstelle	
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)

27.3.6.5 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 Name 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 8 ITSP gleichzeitig aktiv sein. Wertebereich: Provider 1-8
Domain-Name	Gateway-Domännennamen des ITSP. Häufig nicht identisch mit dem Web Domänen-Namen.
Transportprotokoll	Gewünschtes Transportprotokoll. UDP oder TCP können ausgewählt werden.
Transportsicherheit	Die möglichen Werte sind traditionell (UDP oder TCP) für herkömmliche Anrufe mithilfe von UDP/TCP oder sicher (TLS) für sichere Anrufe mithilfe von TLS. Standardwert: traditionell (UDP oder TCP)
Mediensicherheit	Die möglichen Werte sind nur RTP (nur das AVP-Profil wird unterstützt) oder nur SDES (nur das SAVP-Profil wird unterstützt). Standardwert: Nur RTP
Provider-Registrar	
Registrar verwenden	Auszuwählen, wenn die Leitung mit Registrierung arbeitet (Standard = aus).
IP Adresse/Host-Name	Hostname oder IP-Adresse des externen Registrar-Servers.
Port	Portnummer des Registrar-Servers, z. B. 5060. Port 00 eingeben, wenn das ITSP DNSSRV verwendet.
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	

Parameter	Beschreibung
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	
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	
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 eingeben, wenn das ITSP DNSSRV verwendet.
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 (Standard = aus).
IP Adresse/Host-Name	Hostname oder IP-Adresse des STUN-Servers.
Port	STUN-Port-Nummer des STUN-Servers.
Weitere SIP-Provider-Daten	
Erweiterte SIP Provider Daten anzeigen	Bei Aktivierung dieses Flags sind einige zusätzliche Konfigurationsparameter verfügbar, um den SIP-Stack zu kontrollieren und den Inhalt der SIP Header-Felder anzupassen..
CLIP / CLIR	<p>Das System stellt verschiedene Parameter bereit, um das Format von SIP Header-Feldern gemäß den Anforderungen der nativen Leitung zu kontrollieren.</p> <p>Die Inhalte folgender Header-Felder, die den Ursprung eines Anrufs beschreiben, können kontrolliert werden:</p> <ul style="list-style-type: none"> • Von: DisplayPart < sip:UserPart@HostPart • P-Asserted-Identity: DisplayPart < sip:UserPart@HostPart > • P-Preferred-Identity: DisplayPart < sip:UserPart@HostPart >

Parameter	Beschreibung
CLIP ausgehend im Von-Header - Anzeigeteil	<p>Mögliche Einstellungen:</p> <ul style="list-style-type: none"> • Omit - Feld wird ausgelassen • Rufende Nummer - die für einen Teilnehmer konfigurierte Nummer. Sie können in den Richtungsparametern definieren, welche Nummer verwendet wird. • Konto - der Benutzername, der der nativen Leitung zugewiesen ist • Anzeigename
CLIP ausgehend im Von-Header - Benutzerteil:	<p>Mögliche Einstellungen:</p> <ul style="list-style-type: none"> • Rufnummer • Konto
Ausgehender Von-Header - Domänen-/Host-Teil:	<p>Ändern Sie den Domänen-/Host-Teil der URI, die mit der IP-Adresse des Systems ausgefüllt werden soll. Dieser Parameter beeinflusst den Host-Teil von allen drei Header-Feldern: Von:, PAI und PPI.</p> <p>Mögliche Einstellungen:</p> <ul style="list-style-type: none"> • Domain-Name • lokale IP-Adresse • öffentliche IP-Adresse
Umleitung: Von enthält ursprüngliche Rufnummer des Anrufers	<p>Wenn ein ausgehender Anruf aufgrund von Anrufumleitung aufgebaut wird, kann das System Informationen über den ursprünglichen Anrufer angeben.</p> <p>Wenn dies auf „true“ eingestellt ist, sendet das System den ursprünglichen Anrufer (A-Ext) im Header-Feld „Von:“, andernfalls sendet es die Nummer des weiterleitenden Teilnehmers.</p>
Umleitung: PAI enthält ursprüngliche Rufnummer des Anrufers	<p>Wenn ein ausgehender Anruf aufgrund von Anrufumleitung aufgebaut wird, kann das System Informationen über den ursprünglichen Anrufer angeben.</p> <p>Wenn dies auf „true“ eingestellt ist, sendet das System den ursprünglichen Anrufer (A-Ext) im Header-Feld „P-Asserted-Id“, andernfalls sendet es die Nummer des weiterleitenden Teilnehmers.</p> <p>Wenn dieses Flag gesetzt ist, sendet das System den ursprünglichen Anrufer im Header-Feld „P-Asserted_ID:“ und „P-Preferred-ID:“.</p>
CLIP ausgehend im P-Asserted-Id-Header - Anzeigeteil:	<p>Mögliche Einstellungen:</p> <ul style="list-style-type: none"> • Omit - Feld wird ausgelassen • Rufende Nummer - die für einen Teilnehmer konfigurierte Nummer. Sie können in den Richtungsparametern definieren, welche Nummer verwendet wird. • Konto - der Benutzername, der der nativen Leitung zugewiesen ist • Anzeigename

Parameter	Beschreibung
CLIP ausgehend im P-Asserted-Id-Header - Benutzerteil:	Mögliche Einstellungen: <ul style="list-style-type: none"> • Omit - Feld wird ausgelassen • Rufnummer • Konto
CLIP ausgehend im P-Preferred-Id-Header - Anzeigeteil:	Mögliche Einstellungen: <ul style="list-style-type: none"> • Omit - Feld wird ausgelassen • Rufende Nummer - die für einen Teilnehmer konfigurierte Nummer. Sie können in den Richtungsparametern definieren, welche Nummer verwendet wird. • Konto - der Benutzername, der der nativen Leitung zugewiesen ist • Anzeigename
CLIP ausgehend im P-Preferred-Id-Header - Benutzerteil:	Mögliche Einstellungen: <ul style="list-style-type: none"> • Omit - Feld wird ausgelassen • Rufnummer • Konto
CLIP ausgehend im Umleitung-Header - Anzeigeteil:	Mögliche Einstellungen: <ul style="list-style-type: none"> • Omit - Feld wird ausgelassen • Rufende Nummer - die für einen Teilnehmer konfigurierte Nummer. Sie können in den Richtungsparametern definieren, welche Nummer verwendet wird. • Konto - der Benutzername, der der nativen Leitung zugewiesen ist • Anzeigename
CLIP ausgehend im Umleitung-Header - Benutzerteil:	Mögliche Einstellungen: <ul style="list-style-type: none"> • Omit - Feld wird ausgelassen • Rufnummer • Konto
CLIP ausgehend im Verlauf-Info-Header - Benutzerteil:	Mögliche Einstellungen: <ul style="list-style-type: none"> • Omit • Rufnummer
CLIR ausgehend im Von-Header - Anzeigeteil:	Mögliche Einstellungen: <ul style="list-style-type: none"> • Omit • Rufnummer • Konto • Anonymous From: Anonymous <sip: ...@...>
CLIR ausgehend im Von-Header - Benutzerteil:	Mögliche Einstellungen: <ul style="list-style-type: none"> • Rufnummer • Konto • Fully anonymous From: ...<sip:anonymous@anonymous.invalid> • User anonymous From: ... <sip:anonymous@...>

Experten-Modus

Parameter	Beschreibung
CLIR ausgehend Datenschutz-Header	<p>Mögliche Einstellungen:</p> <ul style="list-style-type: none"> • Omit • Id Privacy: id • User Privacy: user • User, id Privacy: user;id
COLP / TIP unterstützt für ausgehende Anrufe:	<p>In ISDN wurde die Funktion COLP (Connect Line Identification Presentation) eingeführt. In SIP wird diese Funktion manchmal als TIP (Termination Identification Presentation) bezeichnet.</p> <p>RFD3324 (Abschnitt 5.) definiert einen Mechanismus zum Transportieren der Identität der annehmenden Partei (C) im Header-Feld „P-Asserted-Identity“ der Antwort 200 OK:</p> <p>Mögliche Einstellungen:</p> <ul style="list-style-type: none"> • COLP unterstützt • COLP nicht unterstützt
Rufnummernformat	
Eingehender Anruf - Rufnummer des Anrufers	<p>Dieses Flag bezieht sich auf die Zieladresse eines Anrufs.</p> <p>Standardmäßig wird dies aus dem Benutzerteil des Header-Felds AN: genommen.</p> <p>Mögliche Einstellungen:</p> <ul style="list-style-type: none"> • Anforderungszeile: INVITE sip: +498970070@... • An-Header-Anzeigeteil An: +498970070 <sip:+ • An-Header-Benutzerteil An: <sip: +498970070@... • P-Called-Party-Id Header-Anzeigeteil P-Called-Party-ID: +498970070 <sip:.. • P-Called-Party-Id Header-Benutzerteil P-Called-Party-ID: <sip: +498970070@..

Parameter	Beschreibung
Eingehender Anruf - Rufnummer des Angerufenen	<p>Dieses Flag bezieht sich auf die Quelladresse eines Anrufs. Standardmäßig nimmt das System den Anrufer aus dem Von-Header-Benutzerteil.</p> <p>Mögliche Einstellungen:</p> <ul style="list-style-type: none"> • automatisch • Von-Header-Anzeigeteil Von: +498970070 <sip:+ • Von-Header-Benutzerteil Von: <sip: +498970070@... • P-Asserted-Id Header-Anzeigeteil P-Asserted-ID: +498970070 <sip:... • P-Asserted-Id Header-Benutzerteil P-Asserted-ID: <sip: +498970070@.. <p>Im automatischen Modus sucht das System zuerst im Benutzerteil von P-Asserted-Identity, falls vorhanden. Falls P-Asserted-Identity nicht vorhanden ist, wird der Benutzerteil des Header-Felds „Von:“ genommen.</p>
Eingehender Anruf - Type of Number (anrufend):	<p>Mögliche Einstellungen:</p> <ul style="list-style-type: none"> • automatisch • international
Eingehender Anruf - Type of Number (angerufen):	<p>Mögliche Einstellungen:</p> <ul style="list-style-type: none"> • automatisch • international • national
Ausgehender Anruf - Type of Number (anrufend):	<p>Mögliche Einstellungen:</p> <ul style="list-style-type: none"> • automatisch • international • national
Ausgehender Anruf - Type of Number (angerufen):	<p>Mögliche Einstellungen:</p> <ul style="list-style-type: none"> • automatisch • international • national
Zuordnung der Anbieternummer:	<p>Mögliche Einstellungen:</p> <ul style="list-style-type: none"> • in jedem Fall • Eingehen, nur angerufen (falls konfiguriert) • aus
CLIP no Screening-Unterstützung:	<p>Mögliche Einstellungen:</p> <ul style="list-style-type: none"> • nicht unterstützt • CLIP eingehend Von / vertrauenswürdige Nummer in PAI • Unterstützt-Keine besondere Behandlung

Experten-Modus

Parameter	Beschreibung
Rufnr. mit internationalem/nationalem Präfix:	Mögliche Einstellungen: <ul style="list-style-type: none"> • Nein • Ja
Angerufene Nummer im E164-Format:	Mögliche Einstellungen: <ul style="list-style-type: none"> • Nein • Ja
Routenoptimierung:	Mögliche Einstellungen: <ul style="list-style-type: none"> • Nicht erlaubt • Erlaubt
MEX-unterstützt:	Mögliche Einstellungen: <ul style="list-style-type: none"> • Nein • Ja
Kontakt-URI enthält:	Dieser Parameter wird verwendet, um den Benutzerteil-Inhalt der Kontakt-URI zu konfigurieren. Contact: sip:UserPart@HostPart:port Mögliche Einstellungen: <ul style="list-style-type: none"> • Rufnummer: Benutzerteil der Kontakt-URI enthält die Rufnummer. • Registration AOR: die Kontakt-URI enthält das Konto = Benutzerteil der Registrierung.
In Kontakt-URI verwendeter TCP-Port:	Dieser Parameter wird verwendet, um den TCP-Port, der im Host-Teil der Kontakt-URI verwendet wird, zu konfigurieren. Contact: sip:UserPart@HostPart:port Mögliche Einstellungen: <ul style="list-style-type: none"> • ephem.src-port: Standardmäßig wird der Port ephemeral tcp src verwendet. • SIP-Server-Port: Der SIP-Server-Port wird in der Kontakt-URI verwendet.
Registrierung	
Registrierungskontakt enthält IP-Adresse:	Mögliche Einstellungen: <ul style="list-style-type: none"> • localIPAddr • domainName
ContactUriWithProtocol:	
BNC-Registrierung (SIPconnect):	Mögliche Einstellungen: <ul style="list-style-type: none"> • normal Registrierung • BNC-Registrierung
Reregistration-Intervall nach Fehler (s):	

Parameter	Beschreibung
Reregistration-Modus:	Mögliche Einstellungen: <ul style="list-style-type: none"> kontinuierlich SIPConnect
Reregistration nach Anruffehler:	Mögliche Einstellungen: <ul style="list-style-type: none"> CallFailureIsNoRegFailure CallFailureIsRegFailure
Sicherheit	
UDP-Modus:	Mögliche Einstellungen: <ul style="list-style-type: none"> symmetrisches UDP asymmetrisches UDP
Approved Peer-Auswahl:	Mögliche Einstellungen: <ul style="list-style-type: none"> nur Trust-konfigurierte Server empfangene Trust-Server in SIP-Reaktionen
Verschiedenes	
Direkte Nutzlast:	
Vermeidung Medien-Neuverhandlung:	
Richtungsattribut ändern:	Mögliche Einstellungen: <ul style="list-style-type: none"> Attribut beibehalten ändern zu sendrecv
Geräuschunterdrückungsattribut:	Mögliche Einstellungen: <ul style="list-style-type: none"> unterstützt nicht unterstützt
Mediasec-Erweiterung:	Mögliche Einstellungen: <ul style="list-style-type: none"> unterstützt nicht unterstützt
SDP-Filter:	Mögliche Einstellungen: <ul style="list-style-type: none"> Standard Kompatibilitätsprofil Offen
UseRouteURIAuthentication:	
100 Rel ignorieren:	
Unterstützung 100rel	
UseViaRPort:	
UPDATE unterstützt:	

Experten-Modus

Parameter	Beschreibung
Unterstützung P-Early-Media-Header:	Mögliche Einstellungen: <ul style="list-style-type: none"> • nicht unterstützt • unterstützt
Session Timer-Unterstützung:	Mögliche Einstellungen: <ul style="list-style-type: none"> • nicht aktiv • Auffrischung Policy Remote
Automatischen Antwort-Timer 183 senden (s):	
UDP-Keep Alive:	Mögliche Einstellungen: <ul style="list-style-type: none"> • UdpKeepAliveON • UdpKeepAliveOFF • SendAliveOptions
Keep-Alive-Intervall für OPTIONEN (s):	
Reregistration nach Fehler OPTIONEN:	Mögliche Einstellungen: <ul style="list-style-type: none"> • NoRegisterOnFailure • RegisterOnFailure
Antworten auf OPTIONEN:	Mögliche Einstellungen: <ul style="list-style-type: none"> • Vollständige Antwort • Ohne Text
Schaltflächen	
ITSP neu starten	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.

Parameter	Beschreibung
STUN-Modus: Statische IP verwenden	Wenn der ITSP eine statische IP-Authentifizierung 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
Standard-STUN-Server	
IP Adresse/Host-Name	IP-Adresse oder Hostnamen des STUN-Servers (z. B. <code>stun.serviceprovider.com</code>). 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 einzutragen.

Experten-Modus

Parameter	Beschreibung
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.: Kennwort, SIP-Kennwort usw.
Kennwort bestätigen	Kennwort, das der ITSP zugewiesen hat. Je nach ITSP werden hierfür unterschiedliche Bezeichnungen verwendet, wie z.B.: Kennwort, SIP-Kennwort usw.

Parameterbeschreibung der Registerkarten:

- **MSN Zugang hinzufügen**
- **MSN Zugang ändern**
- **MSN Zugang löschen**
- **Alle MSN-Einträge löschen**

Parameter	Beschreibung
Internet-Telefonie-Rufnummer / Internet-Telefonie-Teilnehmerrufnummer / 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. (nur Unterstützung für Sprachanrufe, nicht für Fax)
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 Zuordnung der Rufnummern gewünscht wird.

Parameter	Beschreibung
Durchwahlband automatisch den Teilnehmern zuordnen	Wenn ausgewählt, werden die Durchwahlnummern automatisch aufsteigend den internen Rufnummern zugeordnet und es werden entsprechende MSN-Einträge erzeugt.

27.3.6.6 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 Netzwerk 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

27.3.6.7 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.

27.3.6.8 Sprachgateway > SIPQ-Verbindung

Über die SIP-Q-Verbindung werden die Parameter für zwei mögliche externe SIP-Q-Richtungen definiert. Über diese können beliebige externe SIP-Server wie z.B. OpenScape 4000 oder OpenScape Voice angeschaltet werden. Entsprechende Beispiele sind in den vorhandenen Templates eingepflegt.

Parameterbeschreibung der Registerkarten:

- **SIPQ-Verbindung hinzufügen**
- **SIPQ-Verbindung bearbeiten**
- **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-Q-Verbindungen. Wenn vorhanden, ist eine der beiden SIPQ-Verbindungen immer mit der UC Booster Card oder dem UC Booster Server belegt.
Name der Remote-Domäne	Hostname oder IP-Adresse des 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. Wertebereich: 0 oder 1024-65535, Standardwert: 5060
Sicherer Transport	Bei Anschaltung an OpenScape 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. Wertebereich: 0 oder 1024-65535, Standardwert: 5060
Registrierungsintervall (s)	Intervall (in Sekunden), in dem die Registrierung wiederholt wird. Wertebereich: 30 bis 86400, Standardwert: 300
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 bestimmten 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. Wertebereiche: 0 oder 1024-65535

Parameterbeschreibung der Registerkarten:

- **SIPQ-Verbindungsteilnehmer hinzufügen**
- **SIPQ-Verbindungsteilnehmer bearbeiten**
- **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 bestätigen	Wiederholung des Kennworts für den Zugang zum SIP-Server.

27.3.6.9 Sprachgateway > Native SIP Server-Trunk

Hier werden die Parameter für die 10 möglichen externen Native SIP-Richtungen definiert. Über diese können beliebige externe SIP-Server angeschaltet werden.

Parameterbeschreibung der Registerkarten:

- **Native SIP Server-Trunk hinzufügen**
- **Native SIP Server-Trunk bearbeiten**
- **Native SIP Server-Trunk löschen**

Parameter	Beschreibung
Template verwenden	Template, das als Basis verwendet werden soll.
Trunk-Name	Name des externen SIP Servers (Template-Name).
Trunk aktivieren	Die Verbindung zum externen SIP-Server ist aktiviert. Standardwert: Deaktiviert

Experten-Modus

Parameter	Beschreibung
Trunk-ID im System	Auswahl zwischen 10 externen Native SIP Verbindungen. Ausgegraute Einträge sind durch bereits konfigurierte ITSP belegt (max. 8 ITSP möglich - in diesem Fall sind noch 2 Native SIP Verbindungen übrig).
Name der Remote-Domäne	<p>Hostname oder IP-Adresse des externen SIP-Servers. Der Wert ist in der Regel identisch mit dem Wert bei IP-Adresse/Host-Name.</p> <p>Beispiel:</p> <p>Der konfigurierte Name der Remote-Domäne wird im Host-Teil der Header-Felder „Von“ und „PAI/PPI“ verwendet (siehe unten):</p> <p>Von: sip: +49...@DomainName</p> <p>P-Asserted-Identity: sip: +49...@DomainName</p>
Transportprotokoll	Auswahl des UDP- oder des TCP-Protokolls.
Transportsicherheit	Wählen Sie zwischen herkömmlichem UDP oder TCP und sicherem TLS.
Mediensicherheit	Wählen Sie zwischen nur RTP und nur SDES.
SIP-Server	
IP Adresse/Host-Name	Hostname oder IP-Adresse des externen SIP-Servers.
Port	<p>SIP-Port des externen SIP-Servers.</p> <p>Standardwert: 5060, Port 0 eingeben, wenn das ITSP DNSSRV verwendet</p>
Registrar	
Registrar verwenden	Auszuwählen, wenn die Leitung mit Registrierung arbeitet (Standard = aus)
IP Adresse/Host-Name	Hostname oder IP-Adresse des externen Registrar-Servers
Port	<p>Port-Eingabe des externen Registrar-Servers</p> <p>Standardwert: 5060, Port 0 eingeben, wenn DNSSRV verwendet wird</p>
Reregistrierungsintervall	Das Intervall, mit dem eine Registrierung wiederholt wird (Standard = 600)
STUN-Server	
STUN verwenden	Auszuwählen, wenn die Leitung mit STUN arbeitet (Standard = aus)
IP Adresse/Host-Name	Hostname oder IP-Adresse des STUN-Servers
Port	Port des STUN-Servers
Erweiterte SIP-Daten	
Erweiterte SIP-Daten anzeigen	Bei Aktivierung dieses Flags sind einige zusätzliche Konfigurationsparameter verfügbar, um den SIP-Stack zu kontrollieren und den Inhalt der SIP Header-Felder anzupassen.

Parameter	Beschreibung
CLIP / CLIR	<p>Das System stellt verschiedene Parameter bereit, um das Format von SIP Header-Feldern gemäß den Anforderungen der nativen Leitung zu kontrollieren.</p> <p>Die Inhalte folgender Header-Felder, die den Ursprung eines Anrufs beschreiben, können kontrolliert werden:</p> <ul style="list-style-type: none"> • Von: DisplayPart < sip:UserPart@HostPart • P-Asserted-Identity: DisplayPart < sip:UserPart@HostPart> • P-Preferred-Identity: DisplayPart < sip:UserPart@HostPart>
CLIP ausgehend im Von-Header - Anzeigeteil	<p>Mögliche Einstellungen:</p> <ul style="list-style-type: none"> • Omit - Feld wird ausgelassen • Rufende Nummer - die für einen Teilnehmer konfigurierte Nummer. Sie können in den Richtungsparametern definieren, welche Nummer verwendet wird. • Konto - der Benutzername, der der nativen Leitung zugewiesen ist • Anzeigename
CLIP ausgehend im Von-Header - Benutzerteil:	<p>Mögliche Einstellungen:</p> <ul style="list-style-type: none"> • Rufnummer • Konto
Ausgehender Von-Header - Domänen-/ Host-Teil:	<p>Ändern Sie den Domänen-/Host-Teil der URI, die mit der IP-Adresse des Systems ausgefüllt werden soll. Dieser Parameter beeinflusst den Host-Teil von allen drei Header-Feldern: Von:, PAI und PPI.</p> <p>Mögliche Einstellungen:</p> <ul style="list-style-type: none"> • Domain-Name • lokale IP-Adresse • öffentliche IP-Adresse
Umleitung: Von enthält ursprüngliche Rufnummer des Anrufers	<p>Wenn ein ausgehender Anruf aufgrund von Anrufumleitung aufgebaut wird, kann das System Informationen über den ursprünglichen Anrufer angeben.</p> <p>Wenn dies auf „true“ eingestellt ist, sendet das System den ursprünglichen Anrufer (A-Ext) im Header-Feld „Von:“, andernfalls sendet es die Nummer des weiterleitenden Teilnehmers.</p>
Umleitung: PAI enthält ursprüngliche Rufnummer des Anrufers	<p>Wenn ein ausgehender Anruf aufgrund von Anrufumleitung aufgebaut wird, kann das System Informationen über den ursprünglichen Anrufer angeben.</p> <p>Wenn dies auf „true“ eingestellt ist, sendet das System den ursprünglichen Anrufer (A-Ext) im Header-Feld „P-Asserted-Id“, andernfalls sendet es die Nummer des weiterleitenden Teilnehmers.</p> <p>Wenn dieses Flag gesetzt ist, sendet das System den ursprünglichen Anrufer im Header-Feld „P-Asserted_ID:“ und „P-Preferred-ID:“.</p>

Experten-Modus

Parameter	Beschreibung
CLIP ausgehend im P-Asserted-Id-Header - Anzeigeteil:	<p>Mögliche Einstellungen:</p> <ul style="list-style-type: none"> • Omit - Feld wird ausgelassen • Rufende Nummer - die für einen Teilnehmer konfigurierte Nummer. Sie können in den Richtungsparametern definieren, welche Nummer verwendet wird. • Konto - der Benutzername, der der nativen Leitung zugewiesen ist • Anzeigename
CLIP ausgehend im P-Asserted-Id-Header - Benutzerteil:	<p>Mögliche Einstellungen:</p> <ul style="list-style-type: none"> • Omit - Feld wird ausgelassen • Rufnummer • Konto
CLIP ausgehend im P-Preferred-Id-Header - Anzeigeteil:	<p>Mögliche Einstellungen:</p> <ul style="list-style-type: none"> • Omit - Feld wird ausgelassen • Rufende Nummer - die für einen Teilnehmer konfigurierte Nummer. Sie können in den Richtungsparametern definieren, welche Nummer verwendet wird. • Konto - der Benutzername, der der nativen Leitung zugewiesen ist • Anzeigename
CLIP ausgehend im P-Preferred-Id-Header - Benutzerteil:	<p>Mögliche Einstellungen:</p> <ul style="list-style-type: none"> • Omit - Feld wird ausgelassen • Rufnummer • Konto
CLIP ausgehend im Umleitung-Header - Anzeigeteil:	<p>Mögliche Einstellungen:</p> <ul style="list-style-type: none"> • Omit - Feld wird ausgelassen • Rufende Nummer - die für einen Teilnehmer konfigurierte Nummer. Sie können in den Richtungsparametern definieren, welche Nummer verwendet wird. • Konto - der Benutzername, der der nativen Leitung zugewiesen ist • Anzeigename
CLIP ausgehend im Umleitung-Header - Benutzerteil:	<p>Mögliche Einstellungen:</p> <ul style="list-style-type: none"> • Omit - Feld wird ausgelassen • Rufnummer • Konto
CLIP ausgehend im Historie-Info-Header - Benutzerteil:	<p>Mögliche Einstellungen:</p> <ul style="list-style-type: none"> • Omit • Rufnummer

Parameter	Beschreibung
CLIR ausgehend im Von-Header - Anzeigeteil:	<p>Mögliche Einstellungen:</p> <ul style="list-style-type: none"> • Omit • Rufnummer • Konto • Anonymous From: Anonymous <sip: ...@...>
CLIR ausgehend im Von-Header - Benutzerteil:	<p>Mögliche Einstellungen:</p> <ul style="list-style-type: none"> • Rufnummer • Konto • Fully anonymous From: ...<sip:anonymous@anonymous.invalid> • User anonymous From: ... <sip:anonymous@...>
CLIR ausgehend Datenschutz-Header	<p>Mögliche Einstellungen:</p> <ul style="list-style-type: none"> • Omit • Id Privacy: id • User Privacy: user • User, id Privacy: user;id
COLP / TIP unterstützt für ausgehende Anrufe:	<p>In ISDN wurde die Funktion COLP (Connect Line Identification Presentation) eingeführt. In SIP wird diese Funktion manchmal als TIP (Termination Identification Presentation) bezeichnet.</p> <p>RFD3324 (Abschnitt 5.) definiert einen Mechanismus zum Transportieren der Identität der annehmenden Partei (C) im Header-Feld „P-Asserted-Identity“ der Antwort 200 OK:</p> <p>Mögliche Einstellungen:</p> <ul style="list-style-type: none"> • COLP unterstützt • COLP nicht unterstützt
Rufnummernformatierung	
Eingehender Anruf - Rufnummer des Anrufers	<p>Dieses Flag bezieht sich auf die Zieladresse eines Anrufs.</p> <p>Standardmäßig wird dies aus dem Benutzerteil des Header-Felds AN: genommen.</p> <p>Mögliche Einstellungen:</p> <ul style="list-style-type: none"> • Anforderungszeile: INVITE sip: +498970070@... • An-Header-Anzeigeteil An: +498970070 <sip:+ • An-Header-Benutzerteil An: <sip: +498970070@... • P-Called-Party-Id Header-Anzeigeteil P-Called-Party-ID: +498970070 <sip:... • P-Called-Party-Id Header-Benutzerteil P-Called-Party-ID: <sip: +498970070@..

Experten-Modus

Parameter	Beschreibung
Eingehender Anruf - Rufnummer des Angerufenen	<p>Dieses Flag bezieht sich auf die Quelladresse eines Anrufs.</p> <p>Standardmäßig nimmt das System den Anrufer aus dem Von-Header-Benutzerteil.</p> <p>Mögliche Einstellungen:</p> <ul style="list-style-type: none"> • automatisch • Von-Header-Anzeigeteil Von: +498970070 <sip:+ • Von-Header-Benutzerteil Von: <sip: +498970070@... • P-Asserted-Id Header-Anzeigeteil P-Asserted-ID: +498970070 <sip:.. • P-Asserted-Id Header-Benutzerteil P-Asserted-ID: <sip: +498970070@.. <p>Im automatischen Modus sucht das System zuerst im Benutzerteil von P-Asserted-Identity, falls vorhanden. Falls P-Asserted-Identity nicht vorhanden ist, wird der Benutzerteil des Header-Felds „Von:“ genommen.</p>
Kontakt-URI enthält:	<p>Dieser Parameter wird verwendet, um den Benutzerteil-Inhalt der Kontakt-URI zu konfigurieren.</p> <p>Contact: sip:UserPart@HostPart:port</p> <p>Mögliche Einstellungen:</p> <ul style="list-style-type: none"> • Rufnummer: Benutzerteil der Kontakt-URI enthält die Rufnummer. • Registration AOR: die Kontakt-URI enthält das Konto = Benutzerteil der Registrierung.
In Kontakt-URI verwendeter TCP-Port:	<p>Dieser Parameter wird verwendet, um den TCP-Port, der im Host-Teil der Kontakt-URI verwendet wird, zu konfigurieren.</p> <p>Contact: sip:UserPart@HostPart:port</p> <p>Mögliche Einstellungen:</p> <ul style="list-style-type: none"> • ephem.src-port: Standardmäßig wird der Port ephemeral tcp src verwendet. • SIP-Server-Port: Der SIP-Server-Port wird in der Kontakt-URI verwendet.

Parameterbeschreibung der Registerkarten:

- **Native SIP Server-Trunk-Benutzer hinzufügen**
- **Native SIP Server-Trunk-Benutzer bearbeiten**
- **Native SIP Server-Trunk-Benutzer löschen**

Parameter	Beschreibung
Benutzer-ID	Eingabe der Benutzer-ID für den Zugang zum SIP-Server.
Autorisierungsname	Eingabe des Autorisierungsnamens für den Zugang zum SIP-Server.

Parameter	Beschreibung
Kennwort	Eingabe des Kennworts für den Zugang zum SIP-Server.
Kennwort bestätigen	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 > UPO Teilnehmer

Parameterbeschreibung der Registerkarten:

- **Teilnehmer ändern**

Parameter	Beschreibung
Rufnr	Interne Rufnummer des Teilnehmers.
Durchwahl	Durchwahlnummer des Teilnehmers.
Vorname	Frei wählbarer Vorname des Teilnehmers. Wertebereich: max. 32 Zeichen.
Nachname	Frei wählbarer Nachname des Teilnehmers. Wertebereich: max. 32 Zeichen.
Anzeige	Frei wählbarer Name des Teilnehmers. Wird je nach dem für den Anzeigenamen verwendeten Algorithmus standardmäßig mit Vorname und Nachname erstellt. Wertebereich: max. 16 Zeichen
Name	Frei wählbarer Name des Teilnehmers. Wertebereich: max. 16 Zeichen
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.
Gerätetyp	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.

Experten-Modus

Parameter	Beschreibung
Fax DID	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 externe Faxnachrichten vom Teilnehmer empfangen werden können.
Zugang	Anzeige der physikalischen Schnittstelle, an der das Endgerät angeschlossen ist.
ITSP Loc-ID	Die ITSP Standort-ID eines Teilnehmers.
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:

- **UPO 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.
Durchwahl	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-Zone 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-Zone 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.
Gerätetyp	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.

Parameter	Beschreibung
>	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.
Durchwahl	Durchwahlnummer des Teilnehmers.
Vorname	Frei wählbarer Vorname des Teilnehmers. Wertebereich: max. 32 Zeichen.
Nachname	Frei wählbarer Nachname des Teilnehmers. Wertebereich: max. 32 Zeichen.
Anzeige	Frei wählbarer Name des Teilnehmers. Wird je nach dem für den Anzeigenamen verwendeten Algorithmus standardmäßig mit Vorname und Nachname erstellt. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Type	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.

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 DID	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 externe Faxnachrichten vom Teilnehmer empfangen werden können.
ITSP Loc-ID	Die ITSP Standort-ID eines Teilnehmers.
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:

- **Endgeräte Info**

Parameter	Beschreibung
Rufnr	Interne Rufnummer des Teilnehmers.
Anzeige	Name des Teilnehmers.
Gerätetyp	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	

Experten-Modus

Parameter	Beschreibung
>	Springt eine Seite weiter.
<	Springt eine Seite zurück.
>	Springt zum Ende der Liste.
<	Springt zum Anfang der Liste.

Parameterbeschreibung der Registerkarten:

- **Sekundäres Gateway**

Parameter	Beschreibung
Rufnummer	Interne Rufnummer des Teilnehmers.
Name	Name des Teilnehmers.
Knoten-ID	Für jeden Knoten in einem vernetzten System muss eine eindeutige Knoten-ID vergeben werden. Damit sind die einzelnen Knoten im vernetzten System eindeutig identifizierbar.
Notbetrieb	Gibt an, ob die Funktion aktiviert ist.
Rufnr Notbetrieb	Die Rufnummer des Teilnehmers, die bei einem Ausfallereignis verwendet wird.
Duwa Notbetrieb	Die interne Rufnummer des Teilnehmers, der bei einem Ausfallereignis verwendet wird.

Parameterbeschreibung der Registerkarten:

- **Fallback Hosting**

Parameter	Beschreibung
Rufnummer	Interne Rufnummer des Teilnehmers.
Name	Name des Teilnehmers.
Primäre Knoten-ID	Die eindeutige Knoten-ID, für die der Teilnehmer ursprünglich konfiguriert wurde.
Rufnr Notbetrieb	Die Rufnummer des Teilnehmers, die bei einem Ausfallereignis verwendet wird.
Duwa Notbetrieb	Die interne Rufnummer des Teilnehmers, die bei einem Ausfallereignis verwendet wird.

27.3.7.3 Station > Station > Analog Stations

Parameterbeschreibung der Registerkarten:

- **Teilnehmer ändern**

Parameter	Beschreibung
Rufnr	Interne Rufnummer des Teilnehmers. Anmerkung: Rufnummern, die mit einem Stern (*) beginnen, können nicht als Faxziel verwendet werden.
Durchwahl	Durchwahlnummer des Teilnehmers.
Vorname	Frei wählbarer Vorname des Teilnehmers. Wertebereich: max. 32 Zeichen.
Nachname	Frei wählbarer Nachname des Teilnehmers. Wertebereich: max. 32 Zeichen.
Anzeige	Frei wählbarer Name des Teilnehmers. Wird je nach dem für den Anzeigenamen verwendeten Algorithmus standardmäßig mit Vorname und Nachname erstellt. 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.
Gerätetyp	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 DID	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 externe Faxnachrichten vom Teilnehmer empfangen werden können.
Zugang	Anzeige der physikalischen Schnittstelle, an der das Endgerät angeschlossen ist.
ITSP Loc-ID	Die ITSP Standort-ID eines Teilnehmers.
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	

Parameter	Beschreibung
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.
Durchwahl	Durchwahlnummer des Teilnehmers.
Vorname	Frei wählbarer Vorname des Teilnehmers. Wertebereich: max. 32 Zeichen.
Nachname	Frei wählbarer Nachname des Teilnehmers. Wertebereich: max. 32 Zeichen.
Anzeige	Frei wählbarer Name des Teilnehmers. Wird je nach dem für den Anzeigenamen verwendeten Algorithmus standardmäßig mit Vorname und Nachname erstellt. 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.
Gerätetyp	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 DID	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 externe Faxnachrichten vom Teilnehmer empfangen werden können.

Parameter	Beschreibung
Zugang	Anzeige der physikalischen Schnittstelle, an der das Endgerät angeschlossen ist.
ITSP Loc-ID	Die ITSP Standort-ID eines Teilnehmers.
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 > SLC-Rufnummer

Parameterbeschreibung der Registerkarten:

- **Teilnehmer ändern**

Parameter	Beschreibung
Rufnr	Interne Rufnummer des Teilnehmers.
Durchwahl	Durchwahlnummer des Teilnehmers.
Vorname	Frei wählbarer Vorname des Teilnehmers. Wertebereich: max. 32 Zeichen.
Nachname	Frei wählbarer Nachname des Teilnehmers. Wertebereich: max. 32 Zeichen.
Anzeige	Frei wählbarer Name des Teilnehmers. Wird je nach dem für den Anzeigenamen verwendeten Algorithmus standardmäßig mit Vorname und Nachname erstellt. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen

Experten-Modus

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.
Gerätetyp	Anzeige des dem Teilnehmer zugeordneten Endgeräts. Basisstationen werden als S0-Teilnehmer angezeigt.
Zugang	Anzeige der physikalischen Schnittstelle, an der das Endgerät angeschlossen ist.
ITSP Loc-ID	Die ITSP Standort-ID eines Teilnehmers.
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.
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.
Durchwahl	Durchwahlnummer des Teilnehmers.
Vorname	Frei wählbarer Vorname des Teilnehmers. Wertebereich: max. 32 Zeichen.

Parameter	Beschreibung
Nachname	Frei wählbarer Nachname des Teilnehmers. Wertebereich: max. 32 Zeichen.
Anzeige	Frei wählbarer Name des Teilnehmers. Wird je nach dem für den Anzeigenamen verwendeten Algorithmus standardmäßig mit Vorname und Nachname erstellt. 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.
Gerätetyp	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 DID	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 externe Faxnachrichten vom Teilnehmer empfangen werden können.
Zugang	Anzeige der physikalischen Schnittstelle, an der das Endgerät angeschlossen ist.
ITSP Loc-ID	Die ITSP Standort-ID eines Teilnehmers.
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.

27.3.7.7 Teilnehmer > Teilnehmer > IVM/EVM Ports > EVM

Parameterbeschreibung der Registerkarten:

- **Teilnehmer ändern**

Parameter	Beschreibung
Rufnr	Interne Rufnummer des Voicemail-Ports.
Durchwahl	Durchwahlnummer des Voicemail-Ports, sofern vorhanden.
Vorname	Frei wählbarer Vorname des Voicemail-Ports. Wertebereich: max. 32 Zeichen.
Nachname	Frei wählbarer Nachname des Voicemail-Ports. Wertebereich: max. 32 Zeichen.
Anzeige	Frei wählbarer Name des Voicemail-Ports. Wird je nach dem für den Anzeigenamen verwendeten Algorithmus standardmäßig mit Vorname und Nachname erstellt. 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.
Gerätetyp	Bei EVM wird S0-Teilnehmer angezeigt.
Zugang	Anzeige des internen Ports für die Voicemail.
ITSP Loc-ID	Die ITSP Standort-ID eines Teilnehmers.
Teilnehmertyp	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.

Parameter	Beschreibung
<	Springt eine Seite zurück.
>	Springt zum Ende der Liste.
<	Springt zum Anfang der Liste.

27.3.7.8 Teilnehmer > Teilnehmer > Virtuale Teilnehmer

Parameterbeschreibung der Registerkarten:

- **Teilnehmer ändern**

Parameter	Beschreibung
Rufnr	Interne Rufnummer des virtuellen Teilnehmers.
Durchwahl	Durchwahlnummer des virtuellen Teilnehmers.
Vorname	Frei wählbarer Vorname des Teilnehmers. Wertebereich: max. 32 Zeichen.
Nachname	Frei wählbarer Nachname des Teilnehmers. Wertebereich: max. 32 Zeichen.
Anzeige	Frei wählbarer Name des Teilnehmers. Wird je nach dem für den Anzeigenamen verwendeten Algorithmus standardmäßig mit Vorname und Nachname erstellt. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Type	Frei oder Virtueller Teilnehmer (bei Mobility Entry feste Anzeige)
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.
ITSP Loc-ID	Die ITSP Standort-ID eines Teilnehmers.
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.

27.3.7.9 Teilnehmer > Teilnehmer > Teilnehmer-Parameter

Parameterbeschreibung der Registerkarten:

- **Teilnehmer-Parameter ändern**

Parameter	Beschreibung
Teilnehmer - ...	
Typ	Typ des Teilnehmers.
Rufnummer	Interne Rufnummer des Teilnehmers.
Vorname	Frei wählbarer Vorname des Teilnehmers. Wertebereich: max. 32 Zeichen.
Nachname	Frei wählbarer Nachname des Teilnehmers. Wertebereich: max. 32 Zeichen.
Display	Frei wählbarer Name des Teilnehmers. Wird je nach dem für den Anzeigenamen verwendeten Algorithmus standardmäßig mit Vorname und Nachname erstellt. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Durchwahl	Durchwahlnummer des Teilnehmers.
Gerätetyp	Anzeige des dem Teilnehmer zugeordneten 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
Zugang	Anzeige der physikalischen Schnittstelle, an der das Endgerät angeschlossen ist.
Faxnr.	
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.
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 externe Faxnachrichten vom Teilnehmer empfangen werden können.

Parameter	Beschreibung
Mobility/Circuit	
Typ	<p>Typ des Teilnehmers:</p> <ul style="list-style-type: none"> • Mobility Teilnehmer • Virtuelle Teilnehmer • Circuit Teilnehmer • SFB-Teilnehmer • Vertrauenswürdiger externer Teilnehmer: virtueller Teilnehmertyp, der verwendet werden soll, um einen vertrauenswürdigen externen Benutzer zu erstellen
Rufnummer des externen Teilnehmers: Mobil/Circuit/SFB/Trusted	<p>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).</p> <hr/> <p>Anmerkung: Das Feld Rufnummer des vertrauenswürdigen externen Teilnehmers ist obligatorisch. Wenn Sie die Konfiguration mit einem leeren Feld für die Rufnummer des vertrauenswürdigen externen Teilnehmers anwenden, wird folgende Warnmeldung angezeigt: <i>„Die Rufnummer des vertrauenswürdigen externen Teilnehmers darf nicht leer sein!“</i>. Nachdem Sie bei der ersten Meldung auf OK geklickt haben, wird eine zweite Meldung angezeigt: <i>„Die Eingabe konnte nicht verarbeitet werden, bitte überprüfen Sie dies“</i>.</p> <hr/>
Web Feature ID	Die Web Feature ID definiert, wie sich der Teilnehmer beim mobilen Webclient oder Circuit User (Benutzername) anmelden soll. 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	
Teilnehmertyp	Typ des angeschlossenen Endgeräts (Klappliste)
Teilnehmertyp: Standard	Systemtelefone oder analoge Telefone
Teilnehmertyp: Faxnr.	Faxgerät, z.B. kein Aufschalten möglich
Teilnehmertyp: Lautsprecher	Für eine über den a/b-Port realisierte Durchsage-Einrichtung

Experten-Modus

Parameter	Beschreibung
Teilnehmertyp: Anrufbeantworter	<p>Nur bei analog: Ist an dieser Schnittstelle ein Anrufbeantworter angeschlossen, kann mit dieser Einstellung von jedem Endgerät ein Gespräch vom Anrufbeantworter übernommen werden, auch wenn der Anrufbeantworter das Gespräch bereits angenommen hat. Dazu muss am Endgerät eine Taste mit der internen Rufnummer dieses analogen Teilnehmers programmiert werden.</p> <p>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.</p> <p>Nur für virtuelle Ports: Wurde im Manager E ein Teilnehmer ohne Zugang als Typ Anrufbeantworter konfiguriert, muss der Port zusätzlich als virtueller Port konfiguriert sein. Ansonsten ist er im WBM nicht als Teilnehmer sichtbar.</p>
Teilnehmertyp: AB TIn MW LED	<p>Für analoge Telefone (NoFe = Normalfernsprecher) mit Message Waiting-LED</p> <p>Nicht für U.S.</p>
Teilnehmertyp: Teilnehmer mit Impulsschleife	<p>Bei Verwendung eines Impulsschleifen-Endgerätes mit Türöffner-Funktion</p>
Teilnehmertyp: Modem	<p>Bei dieser Einstellung ist kein Umschalten möglich. Sie ist vorgesehen für Modems.</p>
	<p>Wenn ein Fax- oder Modem-Teilnehmer gelöscht wird (Ruf-Nr. und Durchwahl werden gelöscht), muss auch der Stationstyp wieder auf Standard gesetzt werden.</p>
Sprache	<p>Sprache für die Menüsteuerung des Endgeräts (Systemtelefons).</p>
Rufsignalisierung intern	<p>Hier können jedem Teilnehmer eine von insgesamt acht internen Rufsignalisierungen zugewiesen werden. Damit wird zusätzlich zu dem externen Ruf nun ein interner Ruf zugewiesen, der bei einem internen Anruf übertragen wird.</p> <p>Standardwert: Rufart 1</p>
Rufsignalisierung extern	<p>Drei verschiedene Rufarten für die Signalisierung externer Anrufe können hier ausgewählt werden: – Systemtelefone: Rufart 1 = Externer Anruf (z. B. doppelter Ruf), Rufart 2 = Externer Anruf CO 2 (z. B. dreifacher Ruf), Rufart 3 = Externer Anruf CO 3 (z. B. kurz/lang/kurz) – Analoge Endgeräte, Deutschland: Rufart 1 = Externer Anruf, Rufart 2 = Wiederanruf, Rufart 3 = Türklingelruf – Analoge Endgeräte, andere Länder: Rufart 1 = Externer Anruf, Rufart 2 = Externer Anruf, Rufart 3 = Externer Anruf</p> <p>Standardwert: Rufart 1</p>

Parameter	Beschreibung
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 Hotline-Ziel 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 (für IP-System-Clients)	Aktivieren oder Deaktivieren der Verschlüsselung von Telefongesprächen (SPE). Dazu müssen alle beteiligten Teilnehmer SPE aktiviert haben. Standard-Wert: Ein
Payload Security (für TDM-/Analoge Telefone)	Gibt an, ob der spezifische Endpunkt aus Sicht der Infrastruktur gesichert ist oder nicht, da die Payload Security nur für IP-Telefone funktioniert. Wenn dieser Parameter auf „Ein“ gesetzt ist und das Flag SPE Support System aktiviert ist, wird angezeigt, ob der Verbindungspfad zwischen dieser Station und einer IP-Station verschlüsselt ist oder nicht. Wenn der Parameter auf „Aus“ gesetzt ist, werden keine Informationen angezeigt. Standardwert: Aus
MWI-Protokoll	Auswahl des MWI-Protokolls für analoge Teilnehmer. Verfügbar nur für SLMAVx (OpenScape Business X8), 4SLAV onboard und SLAVx OpenScape Business X3, X5.
MWI-Protokoll: Comtel3	ComTel3-Protokoll ausgewählt. Standardwert.
MWI-Protokoll: Hochspannung	Hochspannungsprotokoll ausgewählt. Verfügbar nur für SLMAVx (OpenScape Business X8).
Schaltflächen	
>	Springt zum nächsten Teilnehmer. Wurden zuvor über die Suche -Felder die zum eingegebenen Suchbegriff passenden Teilnehmer gefiltert, können nur diese Teilnehmer angesprungen werden.

Experten-Modus

Parameter	Beschreibung
<	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	
Aufschaltberechtigung ein	Wenn dieses Flag aktiviert ist, kann sich der Teilnehmer in die laufende Verbindung eines internen Teilnehmers aufschalten (bzw. diese überschreiben). 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 deaktiviertem 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. Standardwert: 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 Codeschlusses. Standardwert: Deaktiviert

Parameter	Beschreibung
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, dass das analoge Telefon des Teilnehmers CLIP (Calling Line Identification Presentation) unterstützt. Standardwert: Aktiviert
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. Diese Zeitverzögerung stellt sicher, dass der gerufene Teilnehmer das Leistungsmerkmal "Fangen" aktivieren kann. Dadurch wird die Verfügbarkeit der ISDN-Amtsleitungen reduziert. Standardwert: Deaktiviert
Eintrag in Telefonbuch	Wenn dieses Flag aktiviert ist, werden der Name und die Nummer des Teilnehmers im Systemverzeichnis (einschließlich ODS) 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

Experten-Modus

Parameter	Beschreibung
Keine Rufzuschaltung bei besetzt	<p>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.</p> <p>Standardwert: Deaktiviert</p>
Assoziierte Wahl/ Dienste	<p>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 Codeschlusses.</p> <p>Standardwert: Deaktiviert</p>
Anklopfschutz ein	<p>Bei aktiviertem Flag gilt: Führt der Teilnehmer ein Gespräch, erhält er keine Informationen über weitere kommende Anrufe mittels Anklopfton und Displaymeldung.</p> <p>Standardwert: Aktiviert</p>
Diskret Ansprechen	<p>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.</p> <p>Standardwert: Deaktiviert</p>
Schutz Diskretes Anspr.	<p>Bei aktiviertem Flag kann der Teilnehmer nicht diskret angesprochen werden.</p> <p>Standardwert: Deaktiviert</p>
DTMF-basierte Leistungsmerkmalaktivierung	<p>Nur relevant für Mobility Entry Teilnehmer: Um im Gesprächszustand Leistungsmerkmale aktivieren zu können, muss dieses Flag gesetzt sein. Der Code Receiver bleibt aktiv. (Achtung: begrenzte Ressourcen)</p> <p>Standardwert: Deaktiviert</p>

Parameter	Beschreibung
Headset	<p>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 Berechtigungs freigabe 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.</p> <p>Standardwert: Deaktiviert</p>
Vertretermailbox aktiv	<p>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.</p> <p>Standardwert: Deaktiviert</p>
Anrufprio./Sof. Freiton Anklopfen	<p>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 Externrufen 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 bei Phonemail-Anschlüssen.</p> <p>Standardwert: Deaktiviert</p>
Sprachaufzeichnung	<p>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.</p> <p>Standardwert: Deaktiviert</p>

Experten-Modus

Parameter	Beschreibung
Display-Ausgaben komprimieren	<p>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 Rufnummerninformationen 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.</p> <p>Standardwert: Aktiviert</p>
Türfreigabe, DTMF	<p>Bei aktiviertem Flag kann der Teilnehmer mittels DTMF/MFV-Code die Tür öffnen, wenn am betreffenden Port ein Tür-Relais angeschlossen ist.</p> <p>Standardwert: Deaktiviert</p>
Automatische Rufannahme, CSTA (nur für OpenStage-SIP-Telefone)	<p>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.</p> <p>Standardwert: Aktiviert</p>
Handsfree Mikrofon sperren	<p>Ist das Flag aktiviert, so ist die Nutzung des Freisprechmikrofons nicht möglich. Das Flag wird ausschließlich durch OpenStage-Telefone unterstützt.</p> <p>Standardwert: Deaktiviert</p>
Nummer Anzeige Erzwingen	<p>Bei aktiviertem Flag wird anstelle des Namens die Rufnummer des rufenden Teilnehmers im Display des gerufenen Teilnehmers angezeigt.</p> <p>Standardwert: Deaktiviert</p>
Nutzung (nur für bestimmte Länder)	<p>Mit dieser Aufklappliste kann der Ausgangsstrom der Schnittstellen einer analogen Baugruppe konfiguriert werden (in mA, z.B. 27 mA für China).</p>
Allgemeiner Betriebszustand	<p>In dieser Klappliste kann eine Betriebsart des Teilnehmeranschlusses ausgewählt werden.</p>

Parameter	Beschreibung
Anruferliste ausgeben	Bei aktiviertem Flag wird für den Teilnehmer die Anruferliste in seinem Telefon aktiviert (nur Telefone mit Display). Anrufe, die nicht vom Teilnehmer entgegengenommen wurden, werden mit einem Zeitstempel (Uhrzeit und Datum) versehen und in eine chronologisch sortierte Liste übernommen. Es werden nur Anrufe aufgezeichnet, die auch eine Rufnummer oder einen Namen enthalten. Ruft ein Teilnehmer wiederholt an, so wird nur der Zeitstempel des Eintrages aktualisiert und ein Anrufzähler für diesen Anrufer inkrementiert.
Zentrale Besetztsignalisierung	Für Teilnehmer, die Besetztsignalisierung auf ein zentralisiertes Kommunikationssystem haben, muss dieses Flag gesetzt werden (siehe auch QSIG-Leistungsmerkmale). Gilt nicht in USA. Die Realisierung der zentralen Besetztsignalisierung sieht eine maximale Anzahl von 100 Teilnehmern pro Knoten vor.
Anzeige Notbetrieb-Text	Ist dieses Flag aktiviert, wird im Notbetrieb ein konfigurierbarer Notbetriebs-Text im Display des Telefons angezeigt.
Call Supervision	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 der Call Supervision können Gesprächsaussetzer von bis zu zwei Sekunden auftreten. Standardwert: Deaktiviert
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	

Experten-Modus

Parameter	Beschreibung
Status Message	Nur für System-Clients: Dieses Flag aktiviert den "keep-alive"-Mechanismus für Systemtelefone. Fällt ein Systemtelefon z. B. aus, so wird nach vier 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 Meldungsverkehr 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. Nur für SIP-Clients: Sie müssen ein Kennwort eingeben. Dasselbe Kennwort muss im Gerät verwendet werden.
Neues Kennwort	Kennwort für die Authentifizierung. Nur für SIP-Clients: Wenn das Gerätekennwort noch nicht eingestellt ist, muss dasselbe Kennwort bei „Übernehmen“ verwendet werden, um die Geräteregistrierung zu behalten.
Kennwort bestätigen	Kennwort für die Authentifizierung wiederholen.
SIP User ID / Benutzername	Nur für SIP-Clients: Frei wählbarer Benutzername 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: Mobile Rufnummer	Nur für System-Clients: Dem Teilnehmer ist kein IP-Endgerät fest zugeordnet. Das Leistungsmerkmal wird erst ab dem dritten 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 Failover-Systems 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.
Anrufumleitung	
Ziel Tag	Anzeige der Rufweiserschaltungsziele für kommende externe Rufe am Tag (siehe Wizard User-Telefonie/Rufweiserschaltung)
Ziel Nacht	Anzeige der Rufweiserschaltungsziele für kommende externe Rufe in der Nacht (siehe Wizard User-Telefonie/Rufweiserschaltung).
Ziel Intern	Anzeige der Rufweiserschaltungsziele für kommende interne Rufe (siehe Wizard User-Telefonie/Rufweiserschaltung).
Berechtigung	

Experten-Modus

Parameter	Beschreibung
Tag	Jedem Teilnehmer kann eine Berechtigungsklasse für den Tag zugeordnet werden. Es kann zwischen 15 Berechtigungsklassen gewählt werden (siehe Telefonie/Berechtigungen).
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. Sie können zwischen 32 Anrufübernahmegruppen wählen (120 bei OpenScape Business S; siehe auch Eingehende Anrufe / 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.

27.3.7.10 Teilnehmer > Teilnehmer > UC-Anwendungen

Hier sind die Funktionen der UC-Lösungen UC Smart und UC Suite dargestellt. Es wird empfohlen, die Grundeinstellungen unter "Einrichtung > Grundinstallation > Basisinstallation > Vorkonfigurierte Rufnummern ändern" vorzunehmen.

Abhängig von der verwendeten UC-Lösung werden Ihnen unterschiedliche Funktionen angezeigt.

Parameterbeschreibung der Registerkarten:

- **Teilnehmer ändern**

Parameter	Beschreibung
Rufnr	Rufnummer des Dienstes
Durchwahl	Durchwahlnummer des Dienstes
Vorname	Frei wählbarer Vorname des Dienstes. Wertebereich: max. 32 Zeichen.
Nachname	Frei wählbarer Nachname des Dienstes. Wertebereich: max. 32 Zeichen.
Anzeige	Frei wählbarer Name des Dienstes. Wird je nach dem für den Anzeigenamen verwendeten Algorithmus standardmäßig mit Vorname und Nachname erstellt. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen

Parameter	Beschreibung
Type	Abhängig von der UC-Lösung: UC Smart: MeetMe / Konferenz UC Suite 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) <hr/> Anmerkung: CLIP wird nicht für UC Fax unterstützt. Dies wird nur für Analog-Fax unterstützt. <hr/>
Aktiv	Zeigt an, ob der Dienst betriebsbereit ist.
ITSP Loc-ID	Die ITSP Standort-ID eines Teilnehmers.
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.
<	Springt eine Seite zurück.
>	Springt zum Ende der Liste.
<	Springt zum Anfang der Liste.

27.3.7.11 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)
Maßnahme	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.
Maßnahme	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**

27.3.7.12 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.
Durchwahl	Durchwahlnummernanzeige des Teilnehmers.
(weitere Felder können angezeigt werden)	

27.3.7.13 Teilnehmer > Teilnehmer > Mobility Entry

Es wird empfohlen, mobile Teilnehmer über den Wizard "User Telefonie > Mobiltelefon Integration" einzurichten.

Parameterbeschreibung der Registerkarten:

- **Teilnehmer ändern**

Experten-Modus

Parameter	Beschreibung
Rufnr	Eingabe der internen Rufnummer des Mobility-Teilnehmers (z.B. 777). Diese interne Rufnummer darf noch nicht vergeben sein.
Durchwahl	Eingabe der internen Durchwahlnummer des Mobility-Teilnehmers. Diese interne Durchwahlnummer darf noch nicht vergeben sein.
Vorname	Frei wählbarer Vorname des Mobility-Teilnehmers. Wertebereich: max. 32 Zeichen.
Nachname	Frei wählbarer Nachname des Mobility-Teilnehmers. Wertebereich: max. 32 Zeichen.
Anzeige	Frei wählbarer Name des Mobility-Teilnehmers. Wird je nach dem für den Anzeigenamen verwendeten Algorithmus standardmäßig mit Vorname und Nachname erstellt. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Type	Anzeige des Typs des Mobility-Teilnehmers.
Device-Typ	Anzeige des Systemteletyps, der zur Image-Datei gehört.
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.
Zugang	Anzeige der physikalischen Schnittstelle, an der das Endgerät angeschlossen ist.
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" (Mobility Entry-Teilnehmer ohne myPortal to go) und "automatisch" (interne Rufnummer des Teilnehmers oder MULAP) 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.

Parameter	Beschreibung
>	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.
Knoten ID	Eintrag der Knoten-ID, über die der mobile Teilnehmer extern erreichbar ist.

27.3.7.14 Teilnehmer > Teilnehmer > Circuit-Teilnehmer

Circuit-Teilnehmer können nur über **Einrichtung > Wizards > Circuit: Bearbeiten - Circuit-Benutzerinstanz** hinzugefügt werden

Parameterbeschreibung der Registerkarten:

- **Teilnehmer ändern**

Parameter	Beschreibung
Rufnr.	Eingabe der internen Rufnummer des Circuit-Teilnehmers (z.B. 777). Diese interne Rufnummer darf noch nicht vergeben sein.
DuWa	Durchwahlnummer des Circuit-Teilnehmers.
Vorname	Frei wählbarer Vorname des Teilnehmers. Wertebereich: max. 32 Zeichen.
Nachname	Frei wählbarer Nachname des Teilnehmers. Wertebereich: max. 32 Zeichen.
Anzeige	Frei wählbarer Name des Teilnehmers. Wird je nach dem für den Anzeigenamen verwendeten Algorithmus standardmäßig mit Vorname und Nachname erstellt. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen.
Typ	Anzeige des Typs des Circuit-Teilnehmers.
Circuit-Rufnummer	Die Rufnummer des Circuit-Benutzers.
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.

Parameter	Beschreibung
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.

27.3.7.15 Station > Station > SfB-Benutzer

Parameterbeschreibung der Registerkarten:

- **Teilnehmer ändern**

Parameter	Beschreibung
Rufnr.	Eingabe der internen Rufnummer des Skype for Business Client Mobility-Teilnehmers (z. B. 777). Diese interne Rufnummer darf noch nicht vergeben sein.
DURCHWAHL	Durchwahlnummer für Skype for Business.
Vorname	Frei wählbarer Vorname des Teilnehmers. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Nachname	Frei wählbarer Nachname des Teilnehmers. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Darstellung	Frei wählbarer Name des Teilnehmers. Wird je nach dem für den Anzeigenamen verwendeten Algorithmus standardmäßig mit Vorname und Nachname erstellt. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Typ	Zeigt den Typ des Mobility-Benutzers an, der in diesem Fall immer SfB Station ist.
SfB Rufnummer	Rufnummer des Skype for Business Clients.
Suchen	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 der 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 > 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.
Durchwahl	Durchwahlnummer des Teilnehmers.
Vorname	Frei wählbarer Vorname des Teilnehmers. Wertebereich: max. 32 Zeichen.
Nachname	Frei wählbarer Nachname des Teilnehmers. Wertebereich: max. 32 Zeichen.
Anzeige	Frei wählbarer Name des Teilnehmers. Wird je nach dem für den Anzeigenamen verwendeten Algorithmus standardmäßig mit Vorname und Nachname erstellt. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Gerätetyp	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.

Experten-Modus

Parameter	Beschreibung
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.

27.3.7.17 Teilnehmer > Tastenprogrammierung

Parameterbeschreibung der Registerkarten:

- **Tasten programmieren**

Die Tastenprogrammierung wird nur für UPO-Telefone und HFA-Clients unterstützt. Die Suchfunktion (nach Rufnr., Durchwahl, Vorname, Nachname, Anzeige und Gerätetyp) ist verfügbar.

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
Übernahme 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
Teilnehmer	Anzeige der internen Rufnummer und des Namens des Teilnehmers.

Parameter	Beschreibung
Device-Typ	Anzeige des Telefontyp des Teilnehmers. Device-Typ kann für bereits aktive Teilnehmer nicht geändert werden.
Gerätetyp vom Teilnehmer übernehmen	Auswahl des Teilnehmers, dessen Device-Typ für ausgewählte Teilnehmer übernommen werden soll.
für folgende(n) ausgewählte(n) Teilnehmer	Auswahl des Teilnehmers, dessen Device-Typ übernommen werden soll. Filtern nach verfügbaren Device-Typen der Teilnehmer.

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 Installer's 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).
Verschlüsselung	Encryption ist die Verschlüsselung der Daten auf der Luft-Schnittstelle und kann ein- oder ausgeschaltet werden. Standard: Aktiv

Parameter	Beschreibung
Anmeldefenster	<p>Öffnungszeit des Anmeldefensters für die Anmeldung der DECT-Telefone.</p> <p>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.</p> <p>Standard: 10 Minuten</p>
Echo Handling	<p>Diese Parameter können die unter Leitungen > Parameters/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.</p>
Echo Suppressor	<p>Der Echo Suppressor (ES) schaltet abhängig vom Sendepiegel 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 Sendepiegel des DECT-Telefons nicht gedämpft. Diese Einstellung kann bei analoger Amtsanschaltung und lauter Umgebung bessere Verständlichkeit des Amtsteilnehmers am DECT-Telefons bieten.</p> <p>Standard: Automatisch</p>
Echokompensationsglied	<p>Der Echo Canceller (EC) beseitigt unerwünschte Signalarückflüsse, 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.</p> <p>Standard: Automatisch</p>
Artificial Echo	<p>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.</p> <p>Standard: Automatisch</p>

Parameter	Beschreibung
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-Telefon 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.
Durchwahl	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.

Experten-Modus

Parameter	Beschreibung
Mobilcode	PIN-Code zur Anmeldung des DECT-Telefons. Der Mobilcode muss systemweit eindeutig sein.
Zugang	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 Netzwerk (Knoten-ID = 0), wird die Systemkennung mit 1 vorbelegt. Gehört das Kommunikationssystem zu einem Netzwerk (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.
Zugang	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 -Durchwahlleitung 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.
Type	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: Frei	keine Basisstation angeschaltet.
Name	Name der Basisstation.
Level	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 Rufweiserschaltung.

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 des Gruppenrufs, des Sammelanschlusses, der Basic-MULAP, der Chef-MULAP oder der Sprachbox-Gruppe
Durchwahl	Durchwahlnummer des Gruppenrufs, des Sammelanschlusses, der Basic-MULAP, der Chef-MULAP oder der Sprachbox-Gruppe
Vorname	Frei wählbarer Vorname für den Gruppenruf, den Sammelanschluss, die Basic-MULAP, die Chef-MULAP oder die Sprachbox-Gruppe. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Nachname	Frei wählbarer Nachname für den Gruppenruf, den Sammelanschluss, die Basic-MULAP, die Chef-MULAP oder die Sprachbox-Gruppe. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Anzeige	Name des Gruppenrufs, des Sammelanschlusses, der Basic-MULAP, der Chef-MULAP oder der Sprachbox-Gruppe Wird je nach dem für den Anzeigenamen verwendeten Algorithmus standardmäßig mit Vorname und Nachname erstellt.
Type	Definition des Gruppentyps Standardwert: Gruppe Weitere Informationen siehe: Tabelle: Optionen Typ

Parameter	Beschreibung
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
Mulap als Gruppenmitglied	Wenn dieses Flag aktiviert ist, kann die MULAP-Gruppe als Mitglied unter Gruppen hinzugefügt werden.
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: 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: Eingehende 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: Sie können durch Drücken der MULAP-Taste die belegte MULAP-Leitung für eine Konferenz freigegeben.

Experten-Modus

Parameter	Beschreibung
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.

Tabelle 63: Optionen Typ

Parameter	Beschreibung
<p>Anmerkung: Wenn ein MULAP Mitglied eines linearen Sammelanschlusses, eines zyklischen Sammelanschlusses oder einer einfachen Gruppe ist, sind die folgenden Konvertierungen zulässig:</p>	
<p>1) Gruppe -> Linearer/Zyklischer Sammelanschluss 2) Linearer Sammelanschluss -> Zyklischer Sammelanschluss 3) Zyklischer Sammelanschluss -> Linearer Sammelanschluss</p>	
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 vom Typ 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: RNA	Gruppenruf vom Typ RNA: Ankommende Anrufe werden gleichzeitig bei allen Gruppenmitgliedern signalisiert. Ist ein Mitglied der Gruppe besetzt, wird der gesamte Gruppenruf als besetzt gekennzeichnet (wobei nur die besetzten Gruppenmitglieder den eingehenden Anruf signalisiert bekommen). Anrufer der Gruppe erhalten das Besetztzeichen.

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 eingehenden 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 annehmen	Gruppenruf vom Typ 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 Anklopftton signalisiert.
Typ: Sprachnachricht	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.

27.3.9.2 Kommende Rufe > Gruppen-Teilnehmer

Parameterbeschreibung der Registerkarten:

- **Mitglied bearbeiten**
- **Mitglied löschen**

Parameter	Beschreibung
Gruppe	Nummer (Index) der Gruppe
Gruppenmitglied	Nummer (Index) des Gruppenmitglieds
Rufnummer	Rufnummer des Gruppenmitglieds
Vorname	Frei wählbarer Vorname des Gruppenmitglieds. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen

Experten-Modus

Parameter	Beschreibung
Nachname	Frei wählbarer Nachname des Gruppenmitglieds. Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen
Name	Name des Gruppenmitglieds Wird je nach dem für den Anzeigenamen verwendeten Algorithmus standardmäßig mit Vorname und Nachname erstellt.
MULAP-Name	Name der MULAP (Multiple Line Appearance)-Gruppe. Dies ist der MULAP-Name, der auf dem Display angezeigt wird, wenn diese Teamgruppe aufgerufen wird. Der MULAP-Name ist allen Teamgruppenmitgliedern gemeinsam, die den gleichen Typ haben.
MULAP-Ruf-Nr.	Rufnummer der MULAP-Gruppe
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: Ist dieser Parameter aktiviert, 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 die Basic-MULAP-Leitung gerufen. Chef-MULAP: Ist dieses Flag gesetzt, 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 Sekretär-Funktion einer Chef-MULAP.
Keine automatische Rufannahme kommend (K)	Basic-MULAP und Chef-MULAP: Ist dieses Flag gesetzt, kann ein kommender Anruf nicht durch Abheben des Hörers angenommen werden. Die Annahme eines ankommenden Rufs ist ausschließlich durch Betätigen der MULAP-Taste möglich. Standardwert: Deaktiviert
Automatische Konferenz Freigabe (P)	Basic-MULAP und Chef-MULAP: Ist dieses Flag gesetzt, wird durch Drücken der MULAP-Taste die belegte MULAP-Leitung für eine Konferenz freigegeben. Bei allen weiteren Mitgliedern wird die Freigabe dieser Leitung durch Blinken der MULAP-Taste angezeigt. Durch das Drücken der MULAP-Taste können sie an der Konferenz teilnehmen. Standardwert: Deaktiviert

Parameter	Beschreibung
MULAP-Taste eingerichtet	<p>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.</p> <p>Chef-MULAP: Bei aktiviertem Flag wird bei dem zugehörigen Telefon eine MULAP-Taste eingerichtet. Durch Drücken der Taste erfolgt ein gehender Ruf über die Chef-MULAP-Leitung. Dem Angerufenen wird die Chef-MULAP-Rufnummer im Display angezeigt.</p> <p>Standardwert: Aktiviert</p>
Richtung	Bei einem externen Gruppenmitglied wird die Richtung angezeigt.
Type	Definition des Gruppentyps

27.3.9.3 Kommende Rufe > Team/Top

Für die Erstkonfiguration von Team- und Top-Gruppen wird empfohlen, die Assistenten **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 Gruppe 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.
Vorname	<p>Frei wählbarer Vorname der Team-/Top-Gruppe.</p> <p>Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen</p>
Nachname	<p>Frei wählbarer Nachname der Team-/Top-Gruppe.</p> <p>Wertebereich: max. 16 Zeichen, keine Umlaute oder Sonderzeichen</p>
Name	<p>Name der Team-/Top-Gruppe</p> <p>Wird je nach dem für den Anzeigenamen verwendeten Algorithmus standardmäßig mit Vorname und Nachname erstellt.</p>
Type	Definition des Gruppentyps

Experten-Modus

Parameter	Beschreibung
Typ: Team	Eine Team-Gruppe bietet komfortable Teamfunktionen. Die Teilnehmerrufnummern 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.
Typ: Top	Eine Top-Gruppe bietet komfortable Chef- und Sekretär-Funktionen (Top-Funktion) für bis zu drei Chefs und bis zu drei Sekretäre.
Team als Gruppenmitglied	Dieses Flag ist nur konfigurierbar, wenn die Team-Gruppe Mitglieder mit demselben Teilnehmertyp hat, was zu einer einzelnen MULAP-Gruppe unterhalb dieser Team-Gruppe führt. Wenn dieses Flag aktiviert ist, kann die MULAP-Gruppe als Mitglied unter Gruppen hinzugefügt werden.
Tastenvergabe auf Team	Definition für die Einrichtung der MULAP-Tasten für Mitglieder 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- oder BLF-Modul) des Team-Telefons.
Tastenvergabe auf Team: auf erste freie Tasten	Bei aktiviertem Flag erfolgt eine automatische Einrichtung der MULAP-Tasten auf der ersten freien Taste des Team-Telefons.
Tastenvergabe auf Top	Definition für die Einrichtung der MULAP-Tasten für Mitglieder 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- oder BLF-Modul) des Top-Telefons.
Tastenvergabe auf Top: auf erste freie Tasten	Bei aktiviertem Flag erfolgt eine automatische Einrichtung der MULAP-Tasten auf der ersten freien Taste des Top-Telefons.
Gruppenmitglied	
Gruppe	Nummer (Index) der Gruppe
Mitglieder	Nummer (Index) des Mitglieds innerhalb der Gruppe
Type	Definition des Mitgliedstyps
Ruf-Nr.	Rufnummer des Gruppenmitglieds (ändert sich in einer MULAP-Gruppe in **Ruf-Nr. und ist intern unter dieser **Ruf-Nr. erreichbar.)
Name	Name des Gruppenmitglieds
MULAP-Ruf-Nr.	Rufnummer der MULAP-Gruppe
MULAP-Duwa	Durchwahlnummer der MULAP-Gruppe

Parameter	Beschreibung
MULAP-Name	Name der MULAP-Gruppe. Dies ist der MULAP-Name, der auf dem Display angezeigt wird, wenn diese Teamgruppe aufgerufen wird. Der MULAP-Name ist allen Teamgruppenmitgliedern gemeinsam, die den gleichen Typ haben.
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 Parameters 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 werden einem Mitglied Chef-Funktionen zugewiesen. Beim Abheben des Hörers wird automatisch die Chef-MULAP-Leitung für einen Ruf ausgewählt. Kommende Rufe über die zugehörige Chef-MULAP-Rufnummer werden standardmäßig ausschließlich optisch signalisiert.
Akustischer Ruf(R)	Team-Gruppe und Top-Gruppe: Ist dieser Parameter aktiviert, 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: Ist dieser Flag gesetzt, 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: Ist dieses Flag gesetzt, kann ein kommender Anruf nicht durch Abheben des Hörers angenommen werden. Die Annahme eines ankommenden Rufs ist ausschließlich durch Betätigen der MULAP-Taste möglich. Standardwert: Deaktiviert

Parameter	Beschreibung
Automatische Konferenz Freigabe (P)	<p>Team-Gruppe und Top-Gruppe: Ist dieses Flag gesetzt, wird durch Drücken der MULAP-Taste die belegte MULAP-Leitung für eine Konferenz freigegeben. Bei allen weiteren Mitgliedern wird die Freigabe dieser Leitung durch Blinken der MULAP-Taste angezeigt. Durch das Drücken der MULAP-Taste können sie an der Konferenz teilnehmen.</p> <p>Standardwert: Deaktiviert</p>
MULAP-Taste eingerichtet	<p>Team-Gruppe: Bei aktiviertem Flag wird bei dem zugehörigen Telefon eine MULAP-Taste eingerichtet. Durch Drücken der Taste erfolgt ein gehender Ruf über die MULAP-Leitung des Masters. Dem Angerufenen wird die MULAP-Teilnehmernummer des Masters im Display angezeigt.</p> <p>Top-Gruppe: Bei aktiviertem Flag wird bei dem zugehörigen Telefon eine MULAP-Taste eingerichtet. Durch Drücken der Taste erfolgt ein gehender Ruf über die Chef-MULAP-Leitung. Dem Angerufenen wird die Chef-MULAP-Rufnummer im Display angezeigt.</p> <p>Standardwert: Deaktiviert für alle Mitglieder einer Team-Gruppe. Aktiviert für alle Mitglieder einer Top-Gruppe.</p>
MULAP-Typ	Definition des MULAP-Typs
MULAP-Typ: Basic-MULAP	<p>Kommende Rufe 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.</p>
MULAP-Typ: Chef-MULAP	<p>Alle Mitglieder einer Chef-MULAP sind unter der Chef-MULAP-Rufnummer sowie unter ihren eigenen Teilnehmerrufnummern erreichbar.</p>
Fax Rufnr	Rufnummer der Faxbox des Gruppenmitglieds
Fax DID	Durchwahlnummer der Faxbox des Gruppenmitglieds

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	<p>Nummer (Index) der Anrufübernahmegruppe</p> <p>Wertebereich: 1 bis 32 (120 bei OpenScape Business S)</p>

Parameter	Beschreibung
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.

Experten-Modus

Parameter	Beschreibung
Priorität	<p>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).</p> <p>Standardwert: 1</p>

Parameterbeschreibung der Registerkarten:

- **UCD Gruppen anzeigen**
- **UCD Gruppe ändern**

Parameter	Beschreibung
Rufnummer	Rufnummer der UCD-Gruppe
MSN	Durchwahlnummer der UCD-Gruppe
Name	Name der UCD-Gruppe
Prim. Rufzykl.	<p>Definition des primären Rufzyklus: 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.</p> <p>Standardwert: 3 Zyklen</p>
Sek. Rufzykl.	<p>Definition des sekundären Rufzyklus: 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.</p> <p>Standardwert: 3 Zyklen</p>
Wartende Anrufe	<p>Definition der maximalen Anzahl wartender Anrufe: 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.</p> <p>Standardwert: 10 (Standardwert letzte UCD-Gruppe: 72)</p>
AICC	<p>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.</p> <p>Standardwert: Nein</p>
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.

Parameter	Beschreibung
Ansagewechsel	Definition möglicher Ansagewechsel Standardwert: Einmalig
Ansagewechsel: einzeln	Die in der Warteschlange befindlichen Anrufer erhalten eine einmalige Ansage.
Ansagewechsel: zyklisch	Die letzte und die vorletzte Ansage in der Konfiguration werden zyklisch wiederholt.
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 Ansagen definiert werden. Die Ansagen der Ziele werden dem Anrufer in der Warteschlange nacheinander abgespielt.
Ansageeinrichtungen	Ansage für den betreffenden Ziel-Index.
Wartezeit	Die Ansage kann entweder zyklisch (max. 9 Zyklen mit jeweils 5 sec = 45 sec) oder endlos abgespielt werden. Nach Ablauf dieser Zeit wird dem Anrufer in der Warteschlange die Ansage des nächsten Index vorgespielt (nicht bei endlos). Standardwert: endlos

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.

Experten-Modus

Parameter	Beschreibung
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 > Rufweiserschaltungen

Parameterbeschreibung der Registerkarten:

- **Rufzielliste - Definition**

Parameter	Beschreibung
Rufzielliste	Auswahl der zu bearbeitenden Rufzielliste. Wertebereich: 1 bis 740
Rufweiserschaltung 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.	
Ziel 1 - 4: Kein Eintrag	Rufziel wird übersprungen.
Ziel 1 - 4: Externes Ziel	Richtung und externe Rufnummer mit Amtskennzahl.
Ziel 1 - 4: * Angewählter Teilnehmer	Angerufener Teilnehmer.
Ziel 1 - 4: ** Benutzer definiert	Ziel der Anrufumleitung nach Zeit (falls eingerichtet).
Ziel 1 - 4: #9 Systemsuchlauf	Nächster verfügbarer Teilnehmer (außer Chef-Nebenstelle).
Ziel 1 - 4: #201 - #260	Anrufverteilung (UCD-Gruppe).
Ziel 1 - 4: #801 - #817	Ansagegerät.
Ziel 1 - 4: 100, 101, ...	Rufnummer eines Teilnehmers oder einer Gruppe (z. B. Sprachbox)
Die Rufweiserschaltung erfolgt immer nach	Zeit, nach der ein Anruf an das nächste Rufziel weitergeschaltet wird. Bei UCD-Gruppen folgt die Weiserschaltung den Mechanismen der primären und sekundären Rufzyklen (siehe UCD-Gruppen). Wertebereich: 5/10/15/...75 s, Standardwert: 15 s

Parameter	Beschreibung
Anrufumleitung	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 Rufweitschaltungszeit 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.
Typ	Teilnehmer-Typ, z. B. U _{P0} , System-Client, AB, ISDN, SIP.
Tag	Nummer der Rufzielliste, für kommende externe Anrufe während der Arbeitszeiten (Tagschaltung) Standardwert: 14
Nacht	Nummer der Rufzielliste für kommende externe Anrufe bei aktivierter Nachtschaltung Standardwert: 15
Intern	Nummer der Rufzielliste für kommende interne Anrufe 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 externe Anrufe während der Arbeitszeiten (Tagschaltung)
Nacht	Rufzielliste ist für kommende externe Anrufe bei aktivierter Nachtschaltung
Intern	Rufzielliste ist für kommende interne Anrufe
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-SI-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.
Kennz.	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. Wenn CSTA-Anwendungen verwendet werden, sollte der Wert für diesen Parameter festgelegt werden.

Parameter	Beschreibung
Richtung	Anzeige oder Auswahl der Richtung, die der Leitung zugeordnet ist (keine oder Ltg. Grp 1 bis Ltg. Grp 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.
Type	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-SI-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
Nummer	Anzahl der hinzuzufügenden Leitungen.

Parameterbeschreibung der Registerkarten:

- **Rufrichtung ändern**

Parameter	Beschreibung
Ltg.	Anzeige der Leitungsnummer.
gehend	Ausgehende Anrufe können in der Leitung getätigt werden. <hr/> Anmerkung: Das Absetzen von Notrufen ist möglich, auch wenn das Flag deaktiviert ist. <hr/>
kommend	Eingehende Anrufe können auf der Leitung entgegengenommen werden.

Experten-Modus

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).
Kennz.	Anzeige oder Eingabe der Richtungskennzahl
Richtung	Anzeige oder Auswahl der Richtung, die der Leitung zugeordnet ist (keine oder Ltg. Grp 1 bis Ltg. Grp 12).
Rufzuordnung Leitung	
Tag Ruf-Nr.	Rufnummer für nicht durchwahlfähige kommende Verbindung am Tag
Nacht Ruf-Nr.	Rufnummer für nicht durchwahlfähige, eingehende 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 Primärmultiplexanschluss 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: Unten	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-Länge: 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

Parameter	Beschreibung
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
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.

Parameterbeschreibung der Registerkarten:

- **Rufrichtung ändern**

Parameter	Beschreibung
Ltg.	Anzeige der Leitungsnummer.
Gehend	Ausgehende Anrufe können in der Leitung getätigt werden.
Kommend	Eingehende Anrufe können auf der Leitung entgegengenommen werden.

27.3.10.2 Trunks/Routing > Trunk group

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
Ortskennzahl	Anzeige der Ortsnetzkenzahl 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	
Ländervorwahl	Dient zur Wahlbewertung bei kommenden Rufen. Ländervorwahl ohne führende Nullen (z.B. 1 in USA, 49 in Deutschland)
Ortskennzahl	Dient zur Wahlbewertung bei kommenden Rufen. Ortsnetzkenzahl 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.

Parameter	Beschreibung
Anlagenrufnummer - gehend	
Info: Änderungen bei den Anlagerufnummern 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.
Ortskennzahl	Dient zur Anruferidentifizierung bei gehenden Rufen. Die hier angegebene Ortsnetzkenzahl (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 Ruf-Nr.	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.
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)	

Parameter	Beschreibung
MEX-Nummer	<p>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.</p> <p>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.</p>
Vertrauenswürdiger externer Benutzer	
Vertrauenswürdiger externer Benutzer	Benutzer, der einer externen Kooperationsplattform wie MS Teams zugewiesen werden kann, um Anrufe zu tätigen.

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). Außerdem darf kein Abwurfplatz für die Tag- und Nachtschaltung eingetragen sein (siehe "Abwurf/VPL").

Parameter	Beschreibung
Üb.-Dienst 3,1 kHz Audio	<p>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 müssen als Datendienst gekennzeichnet werden. Um Probleme beim FAX-Betrieb zu vermeiden, sollte dieses Flag gesetzt sein.</p> <p>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.</p>
Rtg.-Präfix ergänzen kommend	Mit aktivierter Option wird bei Systemtelefonen bei kommender Belegung die Rufnummerndarstellung um die Richtungskennzahl ergänzt.
Rtg.-Präfix ergänzen gehend	<p>Mit aktivierter Option wird bei gehender Belegung die Rufnummerndarstellung um den AccessCode ergänzt.</p> <p>Info: Änderungen des Parameters bewirken eine Modifizierung der Anruferidentifizierung und müssen mit den Netzprovidern abgestimmt sein. (Clip no screening)</p>
Rufnr. mit internationalem / nationalem Präfix	<p>Ist dieses Flag aktiviert, muss für den ITSP die nationale bzw. die internationaler Kennziffer der Rufnummer vorangestellt werden (z.B. 02302...., 00492302...).</p> <p>Standard: Aktiviert</p>
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.

Parameter	Beschreibung
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 verwenden	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 "Direkt 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.
Name im Amt	Dieses Flag ist für Ämter konfiguriert, die den Anrufernamen unterstützen.
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.
Amtsruftpause	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. Anderenfalls erfolgt keine Rufweitzerschaltung. 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.

Parameter	Beschreibung
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, Ortsnetzkenzahl 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:
Feld Nr-Typ, gehend: unbekannt	Nur Durchwahlnummer (StandardEinstellung)
Feld Nr-Typ, gehend: Anlagenrufnummer	Anlagenrufnummer + Durchwahlnummer
Feld Nr-Typ, gehend: Ortskennzahl	Ortsnetzkenzahl + Anlagenrufnummer + Durchwahlnummer
Feld Nr-Typ, gehend: Ländervorwahl	Ländervorwahl + Ortsnetzkenzahl + Anlagenrufnummer + Durchwahlnummer
Feld Nr-Typ, gehend: Intern	nur für vernetzte Systeme: bei einem geschlossenen Rufnummernplan soll u.U. kein Nummern-Präfix ergänzt werden. Hier wird eine Rufnummernergänzung unterdrückt.

Experten-Modus

Parameter	Beschreibung
Rufnummerentyp	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.
Rufnummerentyp: 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.
Rufnummerentyp: 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.
Rufnummerentyp: 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	
Richtung ändern	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" abgewickelt werden. Bei Rückweisung von "Partial Rerouting" wird auf "Forward Switching" zurückgegriffen.
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.

Parameter	Beschreibung
Rerouting aktiv: Immer	Wenn das Setup für den eingehenden Anruf auf der gleichen Leitung wie die Ziel-Route der Anrufumleitung eintrifft, wird der Anruf vom Kommunikationssystem abgewiesen (Rufumleitung wird verwendet), wenn diese Option aktiviert ist. Bei vernetzten Systemen muss diese Option in beiden vernetzten Kommunikationssystemen immer gleich aktiviert werden.

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	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.

Parameter	Beschreibung
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.
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-Info sollte dann unterdrückt werden, wenn Probleme bei der externen Anrufumleitung (AUL ext.) auftreten.
With sending complete	Ist dieses Flag gesetzt, wird die optionale Information "Alle Ziffern gesendet" vom System ausgegeben, nachdem alle gewählten Ziffern ausgesendet wurden.
Interner Anruf wie externer	Ist dieses Flag gesetzt, werden netzinterne Anrufe analog zu externen Anrufen akustisch signalisiert.
Ohne autom. Rückruf	Ist dieses Flag gesetzt, wird einem ankommenden ISDN-Ruf mit CCNR (Call Completion on No Reply) signalisiert, dass das System einen Rückrufwunsch entgegen nehmen kann. Das bedeutet, der Anrufer kann einen Rückruf einleiten, wenn der Teilnehmer sich nicht meldet. In einigen Fällen wird diese Meldung vom ISDN-Provider nicht unterstützt. In diesem Fall muss der Schalter aktiviert werden, um das Aussenden von CCNR seitens des Systems zu unterdrücken.

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	<p>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.</p> <p>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.</p> <p>Wertebereich: 1 bis 255</p>
Gruppennummer	<p>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.</p> <p>Wertebereich: 1 bis 40</p>
Anlagenübergreifende Besetztsignalisierung	
Anlagen-Nr. Zielsystem	<p>Mit diesen Daten wird ein Kommunikationssystem definiert, das die zentrale Besetztsignalisierung realisiert. Dies kann sowohl die Hauptanlage als auch eine Untereinlage sein.</p> <p>Anlagennummer des Kommunikationssystems, das für die zentrale Besetztsignalisierung eingerichtet ist.</p> <p>Wertebereich: 1 bis 255</p>
Rufnr. Zielsystem	<p>Rufnummer des Kommunikationssystems, das für die zentrale Besetztsignalisierung 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!</p> <p>Beispiel: Die Rufnummer des Zielsystems sei: 999 Der Wahlplaneintrag muss dann sein: -999 (und nicht -999XXX und nicht -999Z).</p>
Verbindungsdaten-Routing	
Rufnr. Zielsystem	<p>Mit diesen Daten wird ein Kommunikationssystem definiert, das die zentrale Verbindungsdatenerfassung realisiert. Dies kann sowohl die Hauptanlage als auch eine Untereinlage sein.</p> <p>Rufnummer des Kommunikationssystems, das als zentrale Erfassungsstelle eingerichtet ist (siehe auch den Hinweis zu Ruf-Nr. Zielsystem, weiter oben).</p>

27.3.10.4 Leitungen/Routing > 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 Amtes 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) S₀-Amtsleitung
- 4) S_{2M}-Querleitung (nur Slave-Konfiguration)
- 5) S₀-Querleitung

Parameterbeschreibung der Registerkarten:

- **ISDN-Takt**

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 (Classes of Service)

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
Rufnr., 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 Berechtigungsgruppen 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

Parameter	Beschreibung
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: Uneingeschränkt	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 Berechtigungsgruppen 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: Halbamts	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

Parameter	Beschreibung
Berechtigungsgruppe: Verbotliste	Der Teilnehmer darf die in der Verbotliste definierten externen Rufnummern nicht wählen. Ist keine Rufnummer eingetragen gilt Vollamtsberechtigung. Standardwert: Default in Berechtigungsgruppe 3, 5, 6
Berechtigungsgruppe: Uneingeschränkt	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 Berechtigung > Erlaubnislisten

Parameterbeschreibung der Registerkarten:

- **Kurzwahlziele 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) 0800xxxx-Nummern zu berechtigen, muss hier lediglich die 0800 eingegeben 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 > Verbotlisten

Parameterbeschreibung der Registerkarten:

- **Kurzwahlziele anzeigen**
- **Rufnummer hinzufügen**
- **Auswertungsfilter ändern**

Parameter	Beschreibung
Liste 1-6	Anzeigen/Hinzufügen/Ändern/Löschen einer verbotenen Rufnummer. Die Verbotliste enthält die Rufnummern, die der Teilnehmer nicht anrufen kann. Es können bis zu 6 Verbotlisten erstellt werden. Die 1. Verbotliste kann dabei 50 Einträge enthalten, die übrigen 5 Listen jeweils bis zu 10 Einträge.

Parameter	Beschreibung
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) 0900xx-xer-Nummern durch die Teilnehmer zu verhindern, muss hier lediglich die 0900 eingegeben 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.
Auswertungsfiler ändern	
Über die Auswertungsfiler 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 Auswertungsfiler 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 > Blacklist

Parameterbeschreibung der Registerkarten:

- **Liste Anzeigen**
- **Rufnummer hinzufügen**

Parameter	Beschreibung
Rufnummer	Rufnummern können bis zu 25 Stellen (Ziffern 0 bis 9 sowie das Zeichen „+“) umfassen. Das Zeichen „+“ bezieht sich auf das internationale Präfix, das im System konfiguriert ist, und muss an erster Stelle eingegeben werden. Das erste Zeichen kann das Pluszeichen („+“) oder eine beliebige Ziffer sein. Die Telefonnummern werden in der Blacklist numerische sortiert. Blacklist-Einträge müssen im internationalen (z.B. 004989) oder im kanonischen internationalen Format (z.B. +4989) eingegeben werden.
Anonyme Anrufe blockieren	Wenn Sie dieses Flag aktivieren, werden Anrufe ohne Anrufer-Nummer oder mit Anrufer-Nummer, aber eingeschränkter Darstellung blockiert.
Blacklist Funktion	Durch Aktivieren dieses Flags werden die hinzugefügten Rufnummern blockiert. Die Blacklist-Funktion basiert ausschließlich auf der vom Anbieter angegebenen Rufnummer des Anrufers.

27.3.11.7 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.

27.3.11.8 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 Gruppenzuordnung	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. Be im 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. Wertebereich: 1 - 64

Parameter	Beschreibung
Zuweisung KWZ-Bereich zu VBZ-Gruppe	<p>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 der VBZ-Gruppe überschneiden. Es ist jedoch nicht zulässig, einzelne KWZ in den VBZ-Gruppen und mehrere KWZ-Bereiche in einer VBZ-Gruppe einzutragen. Beispielsweise ist Folgendes zulässig: CON 1: 0-99; CON 2: 50-150; CON 3: 200-500. Und Folgendes ist nicht zulässig: CON 1: 0, 5, 10; CON 2: 50-100, 300-500.</p> <p>Wertebereich: 0-7999</p>

27.3.11.9 Berechtigungen > CON Matrix

Parameterbeschreibung der Registerkarten:

- **VBZ-Matrix ändern**

Parameter	Beschreibung
VBZ-Matrix	<p>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.</p>
Raster	<p>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.</p>
Alles sperren	<p>Die VBZ-Matrix unterdrückt den Verkehr zwischen Teilnehmern/ Leitungen innerhalb einer Gruppe (Teilanlage) und zwischen den Gruppen.</p>
Alles freigeben	<p>Die VBZ-Matrix erlaubt den Verkehr zwischen Teilnehmern/ Leitungen innerhalb einer Gruppe (Teilanlage) und zwischen den Gruppen.</p>

Parameter	Beschreibung
Nur guppenintern	Die VBZ-Matrix erlaubt den Verkehr nur zwischen Teilnehmern/ Leitungen innerhalb einer Gruppe (Teilanlage).

27.3.11.10 Berechtigungen > Automatische Nachtschaltung

Parameterbeschreibung der Registerkarten:

- **Alle Tage anzeigen**
- **Tag ändern**

Parameter	Beschreibung
Montag, Dienstag, Mittwoch, Donnerstag, Freitag, Samstag, Sonntag, Sondertag	Tag, der über den Zeitplan eingerichtet wird. 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.
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.
Kopierdienst	Sie können die eingerichteten Zonen auf einen oder mehrere andere Tage kopieren, indem Sie den gewünschten Tag markieren, auf den Sondertag, indem Sie die entsprechende Flagge markieren, auf alle, indem Sie Alle markieren . Wenn Sie auf Übernehmen klicken, werden die Zoneneinstellungen der ausgewählten Tage mit den Zonen des aktuellen Tages überschrieben.

27.3.11.11 Berechtigungen > Sondertage

Parameterbeschreibung der Registerkarte:

- **Sondertage 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
Ansageart	Mit dem Typ des Ankündigungsparameters können Sie zwischen drei möglichen Optionen wählen. Die Musikeinspielung kann dabei intern oder von einer externen Quelle erfolgen.
Ansageart: Keine	Wählen Sie diese Option aus, wenn keine Wiedergabe erfolgen soll.
Ansageart: Start/Stopp	Wählen Sie diese Option aus, wenn eine einmalige Wiedergabe erfolgen soll.
Ansageart: Kontinuierlich	Wählen Sie diese Option aus, wenn eine kontinuierliche Wiedergabe erfolgen soll. Diese Option wird in eingebetteten Systemen nicht unterstützt.

Parameterbeschreibung der Registerkarten:

- **Wartemusik bearbeiten**

Parameter	Beschreibung
MOH Typ	Mit dem Typ des MOH-Parameters können Sie zwischen drei möglichen Optionen wählen. Die Musikeinspielung kann dabei intern oder von einer externen Quelle erfolgen.

Parameter	Beschreibung
MOH Typ: Keine Wartemusik	Wurde diese Option gewählt, ist die Wartemusik komplett deaktiviert. Dies gilt nicht, wenn ein externes Gespräch durch Übergabe vor Melden übergeben wird, dann hört der Anrufer das Freizeichen.
MOH Typ: MOH ohne Rufton	Wurde diese Option gewählt, hört der Anrufer bei einer Übergabe ohne Ankündigung während des Übergabevorgangs und während der externe Anruf beim Übergabeziel signalisiert wird Music on Hold.
MOH Typ: MOH mit Rufton	<p>Wurde diese Option gewählt, hört der Anrufer bei einer Übergabe ohne Ankündigung während des Übergabevorgangs Music on Hold. Sobald die Anrufübergabe erfolgt ist und der externe Anruf beim Übergabeziel signalisiert wird, hört der Anrufer das Freizeichen.</p> <p>In einem vernetzten System sollte immer die Option MOH mit Rufton ausgewählt sein, damit sich für den Kunden ein einheitliches Erscheinungsbild ergibt.</p> <p> Wenn der Anrufer über eine ITSP-Verbindung auf das System zugreift, ist diese Option ohne Funktion und der Anrufer hört während der Anrufübergabe Wartemusik.</p>

Zugriff und Typaktivierung über Manager E.

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. Es ist auch möglich, eine MOH für einen Tag und eine Nacht festzulegen. Es ist ein Reset erforderlich.

27.3.12.2 Anschaltungen > Türsprechstelle (Türöffner)

Parameterbeschreibung der Registerkarten:

- **Türsprechstelle ändern**

Parameter	Beschreibung
Teilnehmer	Auswahl des Rufnummer/Anschlussport der Türsprechstelle. Die Sprechstelle an der Eingangstür muss vom Typ NoFe oder NoPort sein.

Parameter	Beschreibung
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 Rufweitschaltungsalgorithmen.
Türöffner	Freischaltung der Türöffnerfunktion. Ein am TFE-S angeschlossener elektrischer Türöffner wird für die Teilnehmer durch setzen 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: Art des Anrufs	Nur für Standard Mailbox: Die Begrüßung hängt vom Status des Teilnehmers ab: Anruf nicht angenommen - Begrüßung 1 / Besetzt - Begrüßung 2
Begrüßung: Keine	Es wird keine Begrüßung abgespielt. Die Mailbox bleibt aber aktiv, z.B. für eine Weiterleitung des Anrufs zum Abwurfplatz.

Parameter	Beschreibung
Aufzeichnung	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 beim 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	Eingehende 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 bis 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.

Experten-Modus

Parameter	Beschreibung
Telephone User Interface (TUI)	Auswahl der Telefonmenüstruktur der Sprachbox (Telephone 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.
Reihenfolge der Datumsansage	Nur sichtbar mit SmartVM TUI: Einstellung der Ansagenreihenfolge für Nachricht, Aufnahmezeitpunkt und Rufnummer des Anrufer (falls bekannt).
Reihenfolge der Datumsansage: Datum nach Nachricht	Nur sichtbar mit SmartVM TUI: Nachricht -- Aufnahmezeitpunkt -- Rufnummer des Anrufer (falls bekannt).
Reihenfolge der Datumsansage: Datum vor Nachricht	Nur sichtbar mit SmartVM TUI: Aufnahmezeitpunkt -- Rufnummer des Anrufer (falls bekannt) -- Nachricht. Für Nachrichten von internen Teilnehmern gilt: Name des internen Teilnehmers (falls vorhanden) -- Aufnahmezeitpunkt -- Rufnummer des Anrufer (falls bekannt) -- Nachricht.
Anzahl der Nachrichten pro Mailbox	Maximale Anzahl der Nachrichten für eine Mailbox. Wertebereich: 0 bis 100, Standardwert: 30
EVM deaktivieren	Ist dieses Flag aktiviert, ist die SmartVM deaktiviert. Standard: deaktiviert
Rückruf von VM nur an bekannte Nummer zulassen	Wenn ein externer BenutzerA einen BenutzerB anruft, BenutzerB eine Anrufweiterleitung an seine Voicemail eingerichtet hat und der externe BenutzerA eine Sprachnachricht hinterlässt, ruft BenutzerB die SmartVM an, gibt sein Passwort ein und wählt während er sich die Nachricht anhört die „8“. Durch die Wahl dieser Ziffer erfolgt ein Rückruf an BenutzerB. Bei aktiviertem Flag erfolgt der Rückruf, wenn die Nummer von BenutzerB zu den bekannten Rufnummern gehört. Bekannte Rufnummern sind die Mobilrufnummer und die private/externe Rufnummer der Profildetails der Benutzerverwaltung (Applications-UC Smart-User Management). Standard: Aktiviert
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

Parameter	Beschreibung
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: Aktiviert
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: Aktiviert
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 bearbeiten Tag**
- **Kurzwahl-/Abwurfziel bearbeiten Nacht**
- **Kurzwahl-/Abwurfziel bearbeiten 3**
- **Kurzwahl-/Abwurfziel bearbeiten 4**

Parameter	Beschreibung
Auswählen	Auswahl eines internen Teilnehmers (1. Hälfte der Liste) oder einer Sprachbox (2. Hälfte der Liste) als Kurzwahlziel oder Abwurfplatz.
Maßnahme	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.
Type	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 Zurücksetzen 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). 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. 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: <ul style="list-style-type: none"> • 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
Allgemeines	
IP-Adresse	IP-Adresse des DSP-Moduls (kann geändert werden, falls die IP-Adresse bereits vergeben ist). Hinweis: Das letzte Oktett der IP-Adresse kann nicht .1 sein (xxx.xxx.xxx.1)

Experten-Modus

Parameter	Beschreibung
Port	Portnummer des DSP-Moduls
Statusanzeige	Dient zur Erkennung der Verfügbarkeit der DSPs Standardwert: Statusmeldungen
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	
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.
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.

Parameter	Beschreibung
Durchschnittl. Verzögerung für Sprache (ms)	<p>Definition der Zeit in Millisekunden, die ein Paket bei IP-basierten Sprachübertragungen durchschnittlich im Jitter-Buffer gehalten werden soll.</p> <p>INFO: Beim Jitter-Buffer-Typ Adaptiv stellt der hier definierte Wert lediglich einen Anfangswert dar.</p> <p>Standardwert: 40</p>
Max. Verzögerung für Sprache (ms)	<p>Definition der maximalen Zeit in Millisekunden für die Verzögerung für Sprache</p> <p>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.</p> <p>Jitter Buffer-Typ Adaptiv: Anzugeben ist, wie viele Millisekunden die Durchschnittsverzögerung für Sprache maximal betragen darf. Ist die tatsächlich gemessene Verzögerung größer, gehen ausgehende Pakete verloren. Bei adaptivem Jitter-Buffer ist 120 ein für die meisten Umgebungen empfehlenswerter Wert.</p> <p>Hinweis: Der Wert muss in jedem Fall größer sein als der im Feld „Durchschnittliche Verzögerung für Sprache (ms)“ eingetragene Wert.</p> <p>Standardwert: 120</p>
Min. Verzögerung für Sprache (ms)	<p>Definition der minimalen Zeit in Millisekunden für die Verzögerung für Sprache</p> <p>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.</p> <p>Standardwert: 20</p>
Paket-Verlust / Verzögerungpräferenz	<p>Definiert wird das Verhältnis Paketverlust zu Laufzeitverzögerungen von Datenpaketen</p> <p>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.</p> <p>Standardwert: 4</p>

Parameter	Beschreibung
Durchschnittl. Verzögerung für Daten (ms)	<p>Definition der durchschnittlichen Verzögerung für Daten in Millisekunden</p> <p>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.</p> <p>Standardwert: 60</p>
Max. Verzögerung für Daten (ms)	<p>Definition der maximalen Verzögerung für Daten in Millisekunden</p> <p>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.</p> <p>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.</p> <p>Standardwert: 200</p>

27.3.14 Statistiken

Unter **Statistiken** sind die Funktionen für die Anzeige von Statistiken zusammengefasst.

27.3.14.1 Statistik > Gateway-Statistik > Mainboard > Device-Statistik

Parameterbeschreibung der Registerkarten:

- **SCN-Statistik anzeigen**
- **LAN-Statistik anzeigen**

Parameter	Beschreibung
Device-Typ	Zeigt die vorhandenen LAN- und SCN-Komponenten (SCN, Switched Circuit Network) an.
Aktuell belegte Ressourcen	Zeigt die aktuell belegten Ressourcen einer Komponente (konfigurierte und verwendete Channels) an.
Summe	Zeigt die Summe der aktuell belegten Ressourcen an.
Autom. Aktualisierung	Die Anzeige wird alle 60 Sekunden automatisch aktualisiert.
Sekunden bis zur nächsten Aktualisierung	Zeigt einen rückläufigen Timer an, beginnend bei 60 Sekunden.

Parameter	Beschreibung
DSS1-Teilnehmer	Sobald ein Mobiltelefon sich im Bereich einer anderen Funkvermittlungsstelle aufhält („Aufenthalts-Cordless-Baugruppe“), wird mittels einer von der Cordless-Baugruppe initiierten DSS1-Verbindung eine Verlängerungsverbindung geschaltet. Der DSS1-Teilnehmer bezieht sich also auf die im Switch eingerichtete Anzahl von Mobiltelefonen oder DSS1-Verbindungen.
HFA / IP-Networking-Sprache	Diese SCN-Komponente zeigt die Anzahl der DSP-Channels an, die besetzt sind, wenn Gateway-Anrufe eingerichtet werden.
Wartemusik	Bei einer IP-Vernetzung mit aktiviertem Leistungsmerkmal DMC Interworking werden Gateway-Verbindungen über sogenannte DMC-Channels realisiert. Aus Anwendersicht handelt es sich beim DMC-Channel um einen Gateway-Channel, der eine Gateway-Verbindung bereitstellt.
SIU	Die Signalling Unit (SIU) reserviert einen DSP-Channel, der zum Erkennen oder Erzeugen von Systemtönen (z.B. DTMF-Töne) verwendet wird.
DMC	Zeigt einen rückläufigen Timer an, beginnend bei 60 Sekunden.
H.323 (RTP)	Zeigt im Falle eines Sprachanrufs die verwendeten Ressourcen an.
T.38-Fax	Zeigt im Falle einer Fax-Verbindung die verwendeten Ressourcen an.
PPP	Zeigt im Falle eines Anlagenanschlusses die verwendeten Ressourcen an.

27.3.14.2 Statistiken > Gateway-Statistiken > 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-Statistiken

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:

- **Systemtexte anzeigen**

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	
Summe	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 > TZustand 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
Richtung	Zeigt den Routennamen an, um einen besseren Hinweis darauf zu erhalten, zu welchem ITSP eine Leitung gehört.
Trunk Number	Leitungskennzahl
Kommentar	Status der Leitung (Angezeigt wird der letzte Zustand der Leitung.) Möglich sind folgende Leitungszustände: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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	
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
Name	Name des Teilnehmers
Durchwahl	Durchwahlnummer des Teilnehmers
Gerätetyp	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.
Zugang	Bei analogen und U _{PO/E} -Telefonen Anzeige der Baugruppe, des Einbauplatzes und der Nummer des Anschlusses. Zusätzliche Anzeige bei U _{PO/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
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
Leistungsmerkmale	
Anrufschutz	Status des Leistungsmerkmals Anrufschutz Standardwert: Aus
Antworttext	Status des Leistungsmerkmals Antworttext Standardwert: Aus

Parameter	Beschreibung
Codeschloss	Status des Leistungsmerkmals Codeschloss Standardwert: Aus
Rufnummerunterdrückung ein	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
Anrufumleitung 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 und 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 Active Directory Integration Service

Die relevanten Funktionen für die Integration von Active Directory sind unter **Active Directory Integration Service** gruppiert.

27.4.2.1 Active Directory Integration Service

Parameterbeschreibung der Registerkarten:

- **Active Directory Integration Service**

Parameter	Beschreibung
Synchronisierungstyp	<p>Dieser Synchronisierungstyp kann die folgenden Werte haben:</p> <ul style="list-style-type: none"> • Frei Es erfolgt keine Synchronisierung des Teilnehmers mit dem Active Directory Service. • Durchwahl Automatische Synchronisierung des Teilnehmers mit Active Directory. Die Durchwahlnummer wird als Synchronisierungsschlüssel verwendet. • erzwungen Manuelle Synchronisierung des Teilnehmers mit einem Active Directory Teilnehmer. Bei erzwungener Synchronisierung ist es möglich, einen Active Directory-Benutzer mit mehreren OpenScape Business Teilnehmern zu synchronisieren. • mulap_member Der automatisch synchronisierte Benutzer ist ein Mitglied einer MULAP Gruppe.
Suche	<p>Die leeren Felder oben auf dem Bildschirm können für das Suchen nach einem bestimmten Benutzer verwendet werden, wenn die Zahl der Benutzer so groß ist, dass sie nicht auf einen Bildschirm passen.</p> <p>In den Feldern Vorname, Nachname, Anzeigename und DID, wird eine Suche „beginnt mit“ durchgeführt. Im Feld Active Directory-Benutzer wird eine Suche „enthält“ durchgeführt. Die Suche beginnt nach Drücken der Schaltfläche Suchen.</p>

Parameter	Beschreibung
Ändern	Sie können diese Schaltfläche verwenden, um die Synchronisierung des angegebenen Benutzers zu konfigurieren. Die verfügbaren Aktionen bei Auswahl von Ändern bestehen aus den folgenden Schaltflächen, die angezeigt werden.
Daten speichern	Sie können einen spezifischen AD-Benutzer auswählen und die Synchronisierung mit dem spezifischen OpenScape Business Teilnehmer erzwingen. Sie können auf diese Weise unterschiedliche Durchwahlnummern mit demselben AD-Benutzer synchronisieren.
Reset	Versuchen Sie, den OpenScape Business Teilnehmer mit irgendeinem Active Directory-Benutzer zu synchronisieren. Diese Aktion kann zum Beispiel verwendet werden, wenn die Benutzersynchronisierung gestoppt wird.
Nicht synchronisieren	Stoppen Sie die Synchronisierung des angegebenen OpenScape Business Teilnehmers. Bereits synchronisierte Daten für den Benutzer werden nicht entfernt, aber die weitere Synchronisierung mit AD wird abgebrochen.

27.4.3 UC Smart

Unter **UC Smart** sind Funktionen von Unified Communications zusammengefasst.

27.4.3.1 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	
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	

Experten-Modus

Parameter	Beschreibung
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.

27.4.3.2 UC Smart > Benutzerverwaltung

Parameterbeschreibung der Registerkarten:

- **Benutzerverwaltung**

Parameter	Beschreibung
Benutzer	Liste aller vorhandenen Teilnehmer, der ausgewählte Teilnehmer muss eine UC User-Lizenz erhalten
Einstellungen	
Benutzer	Anzeige der internen Telefonnummer des Benutzers.
Name	Anzeige des Namens des Benutzers.
Kennwort	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)

Parameter	Beschreibung
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 E-Mail	Aktivierung/Deaktivierung der Email-Benachrichtigung beim Eingang einer neuen Sprachnachricht.
Sichtbarkeit des Anwesenheitsstatus	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

27.4.3.3 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.

27.4.4 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.

27.4.4.1 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.

27.4.4.2 OpenScape Business, UC Suite > Benutzerverzeichnis

Wenn Sie Ihren Vor- und Nachnamen ändern möchten, müssen Sie dies von Ihrem Administrator durchführen lassen. Andernfalls bleiben die Änderungen nach einer Synchronisation nicht erhalten. Synchronisierungen erfolgen beim Neustart des Systems oder bei Änderungen an Einstellungen durch den Administrator.

Ein Teilnehmer, der Mitglied einer MULAP-Gruppe ist, wird nicht im Benutzerverzeichnis angezeigt. Ein Teilnehmer, der Mitglied eines Sammelanschlusses ist, wird im Benutzerverzeichnis angezeigt.

Parameter	Beschreibung
Suche	Suchen Sie nach einem UC Suite-Benutzer.
Symbol für Anwesenheitsstatus	<p>Der Administrator kann den Anwesenheitsstatus für jeden Benutzer ändern und das Datum und die Uhrzeit der Rückkehr im Format Tag-Monat-Jahr (TT.MM.JJ) bzw. 24 Stunden (HH:MM) festlegen.</p> <p>Eine graue Figur ist momentan nicht an UC Suite angemeldet.</p> <hr/> <p>Anmerkung: Jedes Mitglied eines Sammelanschlusses wird als Nutzer des Systemverzeichnisses angesehen und wird ausgegraut dargestellt.</p> <hr/>
Bearbeiten	<p>Einstellungen des ausgewählten UC Suite Benutzers bearbeiten</p> <hr/> <p>Anmerkung: Aufgrund eines bekannten Kompatibilitätsproblems mit einem Browser kann das Layout des Fensters Benutzer bearbeiten bei Verwendung von Firefox variieren. Das Layout passt zu IE/Chrome/Edge.</p> <hr/>
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	<p>Anmeldename, Kennwort, Nachname, Nebenstelle, Vorname, VoiceMail-Nummer, Faxnummer, Assistenten-Rufnummer, E-Mail, Abteilung, Mobiltelefonnummer, Externe Nummer 1/2, Privatnummer (im kanonischen Format, z. B. +49 89 700798765).</p> <p>Das Kennwort gilt für UC Suite Clients.</p>

Parameter	Beschreibung
Persönliche Daten: Eigenes Bild	Wird automatisch skaliert Unterstützte Dateiformate: BMP, JPG/JPEG/JFIFI, PNG Max. Dateigröße: 10MB
Persönliche Daten: Benutzerebene	Nur vom Administrator für Contact Center einstellbar: Wenn der Agent dauerverfügbar sein soll, aktivieren Sie das Kontrollkästchen Dauer verfügbarer 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 Berechtigungslevels (Agent, Supervisor oder Administrator) aus der Aufklappliste Level definiert. Ein Agent mit dem Berechtigungs-Level Supervisor oder ein Administrator verfügt über erweiterte Berechtigungen.
Meine Einstellungen	Benutzerspezifische Einstellungen des Clients.
Meine Einstellungen: Darstellung	Skin-Farben der Benutzeroberfläche; Sprache der Benutzeroberfläche; Verwendung oder Nichtverwendung der klassischen Ansicht für Pop-up-Fenster.
Meine Einstellungen: Benachrichtigungen	Einstellungen für Pop-up-Fenster.
Meine Einstellungen: Anwesenheit	Einstellungen für den Anwesenheitsstatus.
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, Aufzeichnung von Client-Logs aktivieren, Festlegung der Übergabe-Methode, Aufbewahrungsdauer für Journaleinträge (Maximalwert: 30 Tage), Programmierung von Funktionstasten des Telefons, Aktivierung von Live Search und Einbeziehen von LDAP-Kontakten in die Live Search der Verzeichnisse, Festlegen einer Antwortnachricht.
Anrufregeln	Regeln für kommende Rufe
Anrufregeln: Weiterleitungsziele	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	Benachrichtigungsservice für neue Voicemail - siehe Informationen zur E-Mail Adresse unter „Eigene persönlichen Daten“. Voraussetzung: Der Mailserver und die eigene E-Mail-Adresse sind unter Service Center > E-Mail-Weiterleitung konfiguriert. „Gehend“ erzeugt einen Benutzeranruf an die angegebene Telefonnummer (im kanonischen Format). Die SMS-Rufnummer finden Sie unter Meine persönlichen Daten. Informationen zu SMS-Vorlagen finden Sie im Abschnitt in Vorlagen.
Kommunikation: Fax-Benachrichtigung	Benachrichtigungsservice für neue Faxnachrichten – siehe Informationen zur E-Mail Adresse unter „Eigene persönlichen Daten“. Voraussetzung: Der Mailserver und die eigene E-Mail-Adresse sind unter Service Center > E-Mail-Weiterleitung konfiguriert. „Gehend“ erzeugt einen Benutzeranruf an die angegebene Telefonnummer (im kanonischen Format), entweder nur innerhalb der Geschäftszeiten oder 24 Stunden am Tag. Die SMS-Rufnummer finden Sie unter Meine persönlichen Daten. Informationen zu SMS-Vorlagen finden Sie im Abschnitt in Vorlagen.
Kommunikation: Benachrichtigungen über eingangene Anrufe	Benachrichtigungsservice für neue eingangene Anrufe – siehe Informationen zur E-Mail Adresse unter „Eigene persönlichen Daten“. Voraussetzung: Der Mailserver und die eigene E-Mail-Adresse sind unter Service Center > E-Mail-Weiterleitung konfiguriert.
Profile	Profil für persönlichen AutoAttendant
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 übersprungen, 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; andere Benutzer können sehen, mit wem Sie sprechen und Ihr BLF-Layout kopieren.
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.

Parameter	Beschreibung
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 (Anrufweiterleitung bei Nichtannahme) durch myAttendant (für USA)

27.4.4.3 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)
Hinzufügen	Fügen Sie eine neue Abteilung hinzu.
Bearbeiten	Bearbeiten Sie eine ausgewählte Abteilung.
Entfernen	Entfernen Sie die ausgewählten Abteilungen.

27.4.4.4 OpenScape Business, UC Suite > Gruppen

Durch eine Sprachbox-Gruppe (Anrufbeantworter-Gruppe) kann einer bestimmten Gruppe von Teilnehmern 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.

Mit den Favoritengruppen können Sie Gruppen mit Kontakten erstellen und sie den Benutzern zuweisen.

Parameterbeschreibung der Registerkarten:

- **VoiceMail-Gruppen**

- Fax-Gruppe
- Favoritengruppen

Tabelle 64:

Parameter	Beschreibung
VoiceMail-Gruppen	
Bearbeiten	Bearbeiten Sie die ausgewählte VoiceMail-Gruppe
Entfernen	Entfernen Sie die ausgewählten VoiceMail-Gruppen
VoiceMail-Gruppen	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-Gruppe	
Bearbeiten	Bearbeiten Sie die ausgewählte Fax-Gruppe
Fax-Gruppe	Name der Fax-Gruppe
Pilot	Rufnummer der Fax-Gruppe
Anzahl Benutzer	Anzahl der Mitglieder in der Fax-Gruppe
Anzahl Faxnachrichten	Anzahl der neuen Faxnachrichten für die Fax-Gruppe
Mehrere Benutzer	Wenn es sich um eine Fax-Gruppe handelt, wird Ja angezeigt. Andernfalls wird Nein angezeigt.
Favoritengruppen	
Hinzufügen	Fügen Sie eine neue Favoritengruppe hinzu
Bearbeiten	Bearbeiten Sie die ausgewählte Favoritengruppe
Entfernen	Entfernen Sie die ausgewählten Favoritengruppen

Parameter	Beschreibung
Gruppenname	Name der Favoritengruppe
Anzahl der Kontakte	Anzahl der Kontakte, die der Gruppe hinzugefügt wurden
Editierbar	Wählen Sie, ob der Benutzer die Favoritengruppe bearbeiten kann oder nicht.

27.4.4.5 OpenScape Business UC Suite > Templates

Parameterbeschreibung der Registerkarten:

- **SMS-Dienstanbieter**

Parameter	Beschreibung
Hinzufügen	Fügen Sie eine neue Vorlage hinzu. Geben Sie den Namen der Vorlage und den Namen des Autors ein. Im Feld Empfänger, Betreff oder Text können Platzhalter eingefügt werden, die man jeweils unter "VSL-Felder" auswählt.
Bearbeiten	Bearbeiten Sie die ausgewählte Vorlage. Ändern Sie den Namen der Vorlage und den Namen des Autors. Bearbeiten Sie auch die Felder Empfänger, Betreff und Text. Im Feld Empfänger, Betreff oder Text können Platzhalter eingefügt werden, die man jeweils unter "VSL-Felder" auswählt.
Entfernen	Entfernen Sie die ausgewählte Vorlage.
Als Standardeinstellung übernehmen	Legen Sie die ausgewählte Vorlage als Standard fest.

27.4.4.6 OpenScape Business UC Suite > Externes Verzeichnis

Parameterbeschreibung der Registerkarten:

- **Externes Verzeichnis**

Parameter	Beschreibung
Hinzufügen	Manuelles Hinzufügen einzelner Kontakte zum externen Verzeichnis. Die Zeichen müssen dem UTF-8-Format entsprechen
Bearbeiten	Bearbeitung eines ausgewählten Kontakts aus dem externen Verzeichnis.
Entfernen	Entfernung der ausgewählten Kontakte aus dem externen Verzeichnis.

Parameterbeschreibung der Registerkarten:

- **Externes Verzeichnis importieren**

Experten-Modus

Parameter	Beschreibung
Importieren aus	Wählen Sie, ob der Import der Kontaktdaten aus einer lokalen Datei oder aus einem öffentlichen Windows-Ordner erfolgen soll.
Datei-Upload	Klicken Sie auf Datei auswählen , um die Datei auszuwählen, die in das System hochgeladen werden soll.
Öffentlicher Windows-Ordner	Geben Sie den Dateinamen , den Benutzernamen , die Domäne und das Kennwort des öffentlichen Windows-Ordners ein, der in das System hochgeladen werden soll, und klicken Sie zum Testen auf Testen .
Optionen	Dieser Bereich bietet verschiedene Optionen für die Formatierung der zu importierenden csv-Datei. Zusätzlich gibt es eine Option, die die vorhandenen Daten vor der Ausführung des Imports löscht. Eine weitere Option schließlich legt fest, wie Duplikate während eines Imports behandelt werden sollen.

Parameterbeschreibung der Registerkarten:

- **Externes Verzeichnis exportieren**

Parameter	Beschreibung
Exportieren nach	Wählen Sie, wo die exportierte Datei gespeichert werden soll, lokal oder in einem öffentlichen Windows-Ordner.
Öffentlicher Windows-Ordner	Geben Sie den Dateinamen , den Benutzernamen , die Domäne und das Kennwort des öffentlichen Windows-Ordners ein, der in das System hochgeladen werden soll, und klicken Sie zum Testen auf Testen .

27.4.4.7 OpenScape Business UC Suite > Externer Anbieter

Parameterbeschreibung der Registerkarten:

- **LDAP-Provider**

Parameter	Beschreibung
Hinzufügen / Bearbeiten / Entfernen	Hinzufügen, Bearbeiten oder Entfernen der Zugangsdaten des LDAP-Servers.
Name	Name für dieses externe Offline-Verzeichnis
Server / Server-Adresse	DNS-Name oder IP-Adresse des LDAP-Servers.
Port	Portnummer des externen LDAP-Servers
Benutzername	Benutzername für den Zugriff auf den externen LDAP-Server.
Kennwort	Kennwort für den Zugriff auf den externen Exchange-Server.
LDAP Basis-DN	LDAP Base Distinguished Name ein, z.B. dc=example-for-a-domain, dc=net.

Parameter	Beschreibung
TLS	Aktivieren Sie die Verwendung von nur sicheren Verbindungen zum LDAP-Server.
Anrede, Vorname, Nachname, Geschäftlich 1, Geschäftlich 2, Privat, Mobil, Firma, Firmen-Rufnr., Postanschrift, Bundesland oder Region, Land, Postleitzahl, E-Mail, Pager, Faxrufnummer und Ort	<p>Bei der Konfiguration eines externen Offline-Verzeichnisses kann der 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. Geben Sie jeweils die entsprechende Feldbezeichnung des LDAP-Servers ein.</p> <hr/> <p>Anmerkung: Die Zuordnung des LDAP-Feldes hängt vom entsprechenden Feldnamen durch die Verwendung eines externen LDAP-Servers ab.</p> <hr/>

Parameterbeschreibung der Registerkarten:

- **Exchange-PST**

Parameter	Beschreibung
Hinzufügen / Bearbeiten / Entfernen	Hinzufügen, Bearbeiten oder Entfernen 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.
Auth-Methode	<p>Authentifizierungsmethode, die für den Zugriff auf den externen Exchange-Server verwendet werden soll.</p> <p>Sie können zwischen Einfach und OAuth 2.0 wählen.</p>
Server / Server-Adresse	DNS-Name oder IP-Adresse des Exchange-Servers.
Benutzername	Benutzername für den Zugriff auf den externen Exchange-Server.
Kennwort	<p>Kennwort für den Zugriff auf den externen Exchange-Server.</p> <p>Nur sichtbar, wenn die ausgewählte Authentifizierungsmethode Einfach ist.</p>
Mandanten-ID, Anwendungs-ID, Passwort der Anwendungs ID, Umfang	<p>Mandanten-ID, Anwendungs-ID und Passwort der Anwendungs ID für die Anwendung, die in Azure AD für die Exchange Directory Integration registriert wurde. Wenden Sie sich dafür an Ihren Azure AD-Administrator.</p> <p>Umfang, den die Anwendung erfordert (optional). Standardwert: https://outlook.office365.com/.default</p> <p>Nur sichtbar, wenn die ausgewählte Authentifizierungsmethode OAuth 2.0 ist.</p>

Parameterbeschreibung der Registerkarten:

- **Exchange-Kalender-Integration**

Parameter	Beschreibung
Exchange-Kalender-Integration	Bei Abwesenheit des Nutzers dient die Kalenderintegration der automatischen Erstellung von Outlook-Terminen 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 Zugangsdaten eingegeben werden.
Exchange-Kalender-Integration aktivieren	Aktivieren der Exchange-Kalenderintegration
Auth-Methode	Authentifizierungsmethode, die für den Zugriff auf den externen Exchange-Server verwendet werden soll. Sie können zwischen Einfach und OAuth 2.0 wählen.
Server	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 .
Benutzername	Benutzername für den Zugriff auf den externen Exchange-Server.
Kennwort	Kennwort für den Zugriff auf den externen Exchange-Server. Nur sichtbar, wenn die ausgewählte Authentifizierungsmethode Einfach ist.
Mandanten-ID, Anwendungs-ID, Passwort der Anwendungs ID, Umfang	Mandanten-ID, Anwendungs-ID und Passwort der Anwendungs ID für die Anwendung, die in Azure AD für die Exchange Calendar Integration registriert wurde. Wenden Sie sich dafür an Ihren Azure AD-Administrator. Umfang , den die Anwendung erfordert (optional). Nur sichtbar, wenn die ausgewählte Authentifizierungsmethode OAuth 2.0 ist.

27.4.4.8 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	Gruppennummer-ID 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 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
Enddatum	Datum für das Ende der Ausnahme-Regel
Startzeit	Uhrzeit für den Beginn der Ausnahme-Regel
Endezeit	Uhrzeit für das Ende der Ausnahme-Regel
erfolgt	Die Häufigkeit, mit der die Ausnahmeregel eingeplant wird

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.
Gruppennummer	Gruppennummer-ID der UCD-Gruppe, die bei der Grundkonfiguration des Contact Centers eingerichtet wurde.
Allgemeine Einstellungen	
Name der Warteschlange	Name der Warteschlange
Warteschlange aktiv	Definition des Warteschlangenzustands
Warteschlange aktiv: Inaktiv	Die Warteschlange ist nicht aktiv.
Warteschlange aktiv: Aktiv	Die Warteschlange ist aktiv.
Gruppennummer	Gruppennummer-ID der UCD-Gruppe, 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
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

Parameter	Beschreibung
Schwellwert für abgebrochene Anrufe	<p>Schwellwertzeit für abgebrochene Anrufe in Sekunden</p> <p>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.</p> <p>Der Filter für den Schwellwert für abgebrochene Anrufe ist nicht im Übersichtsbericht pro Warteschlange verfügbar.</p> <p>Standardwert: 5 Sekunden</p>
Popup-Fenster aktiviert	<p>Bei aktiviertem Flag erscheint in myAgent bei kommenden Anrufen ein PopUp-Fenster zur Anzeige und Eingabe von Kundendaten.</p> <p>PopUp-Fenster sind erforderlich, um Rückrufe anzunehmen und auszuführen und um Faxe und E-Mails anzunehmen.</p> <p>Standardwert: Deaktiviert</p> <hr/> <p>Anmerkung: Die Benachrichtigungsoption über myAgent > Einrichten > Meine Einstellungen > Benachrichtigungen > Popup-Anwendung für eingehende Anrufe wird durch die Aktivierung des Bildschirm-Popups über WBM > ContactCenter > Warteschlangeneinstellungen außer Kraft gesetzt.</p> <hr/>
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.
Zeitüberschreitung PopUp-Fenster	<p>Screenpop-Timeout in Sekunden.</p> <p>Wenn dieser auf 0 gesetzt ist, fordert myAgent implizit eine Screenpopup-Zeit von 20 Sekunden an.</p> <p>Standardwert: 20 Sekunden</p>
Prioritäten	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.
Warteschlangentiefe-Modus	Definition des Warteschlangentiefe-Modus
Warteschlangentiefe-Modus: Statisch	Falls der Warteschlangentiefe-Modus auf „Statisch“ gesetzt wurde, können WLS und Warteschlangentiefe konfiguriert werden.

Experten-Modus

Parameter	Beschreibung
Warteschlangentiefe-Modus: Keine	Falls die Warteschlangentiefe auf „Keine“ gesetzt wurde, können die WLS-Parameter konfiguriert werden. Dies beeinflusst auch die UCD-Konfiguration, aber die Warteschlangentiefe kann nicht eingestellt werden.
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.
Hinzufügen	Einen neuen Dienst für eingehende E-Mails hinzufügen
Bearbeiten	Einen ausgewählten Dienst für eingehende E-Mails bearbeiten
Entfernen	Den ausgewählten Dienst für eingehende E-Mails entfernen
Auth-Methode	Authentifizierungsmethode, die für den Zugriff auf den Dienst für eingehende E-Mails verwendet werden soll Sie können zwischen Einfach und OAuth 2.0 wählen.
Server	DNS-Name oder IP-Adresse des Dienstes für eingehende E-Mails
Port	Portnummer des Dienstes für eingehende E-Mails
Benutzername	Benutzername für den Zugriff auf den Dienst für eingehende E-Mails
Kennwort	Kennwort für den Zugriff auf den Dienst für eingehende E-Mails Nur editierbar, wenn die ausgewählte Authentifizierungsmethode Einfach ist.
Verwendet SSL-Verbindungen	Aktivieren oder deaktivieren Sie die Verwendung von SSL-Verbindungen entsprechend der Konfiguration des Dienstes für eingehende E-Mails
Mandanten-ID, Anwendungs-ID, Client Secret, Umfang	Mandanten-ID, Anwendungs-ID und Client Secret für die Anwendung, die in Azure AD für die E-Mail-Warteschlangen registriert wurde. Wenden Sie sich dafür an Ihren Azure AD-Administrator. Umfang , den die Anwendung erfordert (optional). Standardwert: https://outlook.office365.com/.default Nur sichtbar, wenn die ausgewählte Authentifizierungsmethode OAuth 2.0 ist.
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.

Parameter	Beschreibung
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	Gruppennummer-ID der UCD-Gruppe, 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	Gruppennummer-ID der UCD-Gruppe, 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	Gruppennummer-ID der UCD-Gruppe, die bei der Grundkonfiguration des Contact Centers eingerichtet wurde.
VIP-Rufliste	Angezeigt werden die in der VIP-Rufliste enthaltenen Anrufer und Rufnummernmuster. Sie können Anrufer und Rufnummernmuster in der VIP-Anrufliste hinzufügen, bearbeiten oder entfernen. 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	Gruppennummer-ID der UCD-Gruppe, die bei der Grundkonfiguration des Contact Centers eingerichtet wurde.
Bevorzugte Agenten	Angezeigt werden die bevorzugten Agenten der in der Kundenliste genannten Anrufer. Sie können einen Agenten hinzufügen, entfernen und seine Priorität ändern. 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
Hinzufügen	Eine neue Contact Center-Pause hinzufügen
Bearbeiten	Eine ausgewählte Contact Center-Pause bearbeiten
Entfernen	Die ausgewählte Contact Center-Pause entfernen
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

Experten-Modus

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
Hinzufügen	Eine neue einfache Nachbearbeitung hinzufügen
Bearbeiten	Eine ausgewählte einfache Nachbearbeitung bearbeiten
Entfernen	Die ausgewählte einfache Nachbearbeitung entfernen
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.

Parameter	Beschreibung
Gruppennummer	Gruppennummer-ID der UCD-Gruppe, die bei der Grundkonfiguration des Contact Centers eingerichtet wurde.
Agentenzuweisung	
Nebenstelle	Anzeige der Durchwahlnummer des Benutzers
Name	Anzeige des Namens des Benutzers.
Agent	Agent, der der Warteschlange zugeordnet ist.
Typ	Agententyp Möglich sind folgende Optionen: <ul style="list-style-type: none"> • Hauptagent: Der Agent erhält Anrufe unabhängig von der Auslastung der Warteschlange. • Agent bei Überlauf: Der Agent erhält Anrufe nur bei Überlauf der Warteschlange.
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
Überlauf nach Sekunden in Warteschlange	Nur für Agent bei Überlauf: Overflow-Zeit 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 Anrufe Anrufe, die über diese Maximalzahl hinausgehen, werden an einen Agenten bei Überlauf weitergeleitet.

27.4.4.9 OpenScape Business UC Suite > Zeitpläne

Parameterbeschreibung der Registerkarten:

- **Bearbeiten/Hinzufügen**

Parameter	Beschreibung
Automatischer Vermittlungsplatz (VPL)	Konfiguration der AutoAttendant-Funktion der UC Suite (Company AutoAttendant)
Zeitplan	Name des Zeitplans
Warteschlange	Name der Warteschlange, der der Zeitplan zugeordnet ist.

Experten-Modus

Parameter	Beschreibung
Gruppennummer	Gruppennummer-ID der UCD-Gruppe, die bei der Grundkonfiguration des Contact Centers eingerichtet wurde.
Bearbeiten / Hinzufügen / Entfernen	Bearbeiten oder Entfernen der ausgewählten Regel oder Hinzufügen einer neuen (öffnet den Regel-Editor)
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.
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)
Enddatum	Ende der Ausnahme (Datum)
Startzeit	Beginn der Ausnahme (Uhrzeit)
Endezeit	Ende der Ausnahme (Uhrzeit)

Parameter	Beschreibung
(Wochentag)	Die Ausnahme soll an einem oder mehreren Wochentagen gelten
erfolgt	Die Häufigkeit, mit der die Ausnahme geplant wird

27.4.4.10 OpenScape Business UC Suite > Datei-Upload

Parameterbeschreibung der Registerkarten:

- **Audiodatei-Manager**

Parameter	Beschreibung
Upload-Ziel	Applikation, für welche die neue Ansage verwendet wird
Upload-Ziel: Automatischer Vermittlungsplatz (VPL)	Ansagen für die automatische Vermittlung
Upload-Ziel: Profile	Ansagen für alle oder einzelne Benutzer von UC Suite
Upload-Ziel: VoiceMail-Begrüßung	Sprachbox-Begrüßungen für alle oder einzelne Benutzer von UC Suite Die Aufzeichnungsdauer für VoiceMail-Begrüßungen ist auf 1 Minute begrenzt.
Upload-Ziel: VM-Gruppenbegrüßung	Begrüßung für eine Gruppen-Sprachbox
no key for: uploader	Die Ansage liegt zum Upload als PCM-Datei 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
WAV-Datei	
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.
Abspielen	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 verfügbar als .ocp Datei
Name	Der Name des zentralen Fax-Deckblatts
Beschreibung	Eine Beschreibung für das zentrale Fax-Deckblatt
Upload	Zentrale Fax-Deckblattdatei hochladen
Bearbeiten	Ausgewählte zentrale Fax-Deckblattdatei bearbeiten
Entfernen	Ausgewählte zentrale Fax-Deckblattdatei entfernen
Als Standardeinstellung übernehmen	Ausgewählte zentrale Fax-Deckblattdatei als Standard festlegen
Dateiname	Angabe des Dateinamens der hochzuladenden Ansage
Erstellungsdatum	Erstellungsdatum der zentralen Fax-Deckblattdatei

27.4.4.11 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
Display	Teilnehmer der ausgewählten Konferenz
Löschen	Die ausgewählten Konferenzen löschen

27.4.4.12 OpenScape Business UC Suite > Standort-Liste

Parameterbeschreibung der Registerkarten:

- **Standort-Liste**

Parameter	Beschreibung
Standort-Name	Standorte im vernetzten Kommunikationssystem (siehe Grundeinstellungen > Gateway-Eigenschaften)

Parameter	Beschreibung
Standort-Adresse	IP-Adresse von UC Booster Card, von UC Booster Server oder des Kommunikationssystems
Standort-Port	Server Port
Standort-IP-Trunks	Standort-IP-Trunks, sofern vorhanden
Online-Status	Verbindungsstatus des Kommunikationssystems am Standort

27.4.4.13 OpenScape Business UC Suite > Server

Parameterbeschreibung der Registerkarten:

- **Allgemeine Einstellungen**
- **Gespräch aufzeichnen**
- **Protokollierung**
- **Benachrichtigungen**
- **Wartung**
- **VoiceMail**
- **Contact Card Mapping**

Parameter	Beschreibung
Bürozeiten	
Startzeit	<p>Beginn der täglichen Bürozeit (Geschäftszeit) Einstellung für den Anwesenheitsstatus der UC Clients Standardwert: 07:00</p> <hr/> <p>Anmerkung: Der Wert muss im 24-Stunden-Format (HH:MM) eingegeben werden.</p> <hr/>
Endezeit	<p>Ende der täglichen Bürozeit (Geschäftszeit) Einstellung für den Anwesenheitsstatus der UC Clients Standardwert: 19:00</p> <hr/> <p>Anmerkung: Der Wert muss im 24-Stunden-Format (HH:MM) eingegeben werden.</p> <hr/>
Kennwortlänge	
Längen	<p>Länge des Kennworts für die UC Clients. Der Mindestwert ist 6. HINWEIS: Durch das Ändern der Kennwortlänge werden die Kennwörter aller Benutzer zurückgesetzt. Standardwert: 6</p>
Rufnummer des Abwurfplatzes	

Experten-Modus

Parameter	Beschreibung
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: Alles anzeigen
Modus Analoger Teilnehmer: Alles 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 angezeigt	Kein analoger Teilnehmer wird im internen Verzeichnis angezeigt.
Nebenstelle	
Max. interne Länge	Maximale Zifferanzahl bei internen Rufnummern Zum Schutz vor Gebührenmissbrauch ist die Wahl längerer interner Rufnummern nicht möglich. Standardwert: 4
Min. externe Länge	Minimale Zifferanzahl bei externen Rufnummern Standardwert: 3
Übergeben	
Normales Vermittlungsplatz-SST	Bei aktiviertem Flag erfolgt die Übergabe eines Anrufs, unabhängig davon, ob das Ziel frei, besetzt oder nicht verfügbar ist. Standardwert: Aktiviert
Journal	
Löschen von Journaleinträgen zulassen	Dieses Flag ermöglicht bzw. verbietet das Löschen von Journaleinträgen durch den Benutzer.
Min. externe Länge	
Faxformat	
Als Faxformat PDF verwenden	Wenn das Flag aktiviert ist, kann das eingegangene Fax im PDF-Format gespeichert werden, andernfalls wird das TIFF-Format verwendet.

Parameter	Beschreibung
Verzeichnisserver	
Langsamer externer Provider	Dieses Flag verbessert die Antwortzeit beim Klicken mit der rechten Maustaste auf eine E-Mail. Auch wenn es aktiviert ist, wird die Suche nach Kontakten nur im übergeordneten Exchange-Verzeichnis und nicht in Unterverzeichnissen durchgeführt.
Länge der Überprüfung	Geben Sie eine 4- bis 8-stellige Ziffer ein, um die Länge der CLI-Nummern für die Suche im LDAP-Verzeichnis von myPortal for Desktop und myPortal for Outlook zu definieren. Die höchste Zahl (8) steht für genauere Suche bzw. bessere Performance des Systems Standardwert: 4
Nach Name wählen – Nur lokale Nebenstelle suchen	Wenn dieses Flag markiert ist, ist die Funktion "Nach Namen wählen" auf den aktiven Knoten beschränkt (lokale Funktion). Wenn dieses Flag nicht markiert ist, bleibt die alte Funktion verfügbar, die alle Benutzer im Netzwerk berücksichtigt, aber die Ansage erst nach der Auswahl eines lokalen Benutzers abspielt.
Der Verzeichnis-Suchcache läuft ab in	Legen Sie die Anzahl der Minuten oder einen Bereich von Minuten fest, in denen der Cache-Speicher bei der Suche nach Kontakten verwendet wird. Sie können einen Minutenbereich von 1-60 Minuten einstellen. Bei einem Wert von "0" ist diese Funktion deaktiviert.
Suchen nach Rufnummer	Wenn dieses Flag aktiviert ist, können Sie in Verzeichnissen nach Telefonnummern suchen.
TLS	
Für Client-Verbindungen TLS verwenden	Aus Netzwerkgründen kann es erforderlich sein, die sichere Client-Server-Verbindung auszuschalten. Das Ändern dieser Einstellung erfordert einen Neustart der UC Applikation. Dies sollte auf sehr spezielle Fälle beschränkt bleiben!
Anwesenheit	
Status „Krank“ ausblenden	Wenn dieses Flag aktiviert ist, steht der Anwesenheitsstatus "krank" nicht zur Verfügung. Standardwert: Deaktiviert
Benutzername	
Bearbeitung des Namens deaktivieren	Wenn dieses Flag aktiviert ist, können Benutzer ihren konfigurierten Vor- und Nachnamen nicht ändern. Standardwert: Deaktiviert
Wandanzeige (Wallboard)	
Wandanzeige deaktivieren	Wenn dieses Flag aktiviert ist, steht die Wandanzeige nicht zur Verfügung.

Experten-Modus

Parameter	Beschreibung
Agentennamen in der Warteschlangen-Bindung von myAgent anzeigen	Ist dieses Flag aktiviert, erscheint gemeinsam mit der Rufnummer eines Agenten auch ein Name, den der Benutzer konfigurieren kann. Ein Benutzer zeigt "Hotdesk" an, wenn er eine andere als seine eigene Nebenstelle verwendet. Standardwert: Deaktiviert.
Gespräch aufzeichnen	
Gespräch aufzeichnen	Bei aktiviertem Flag ist das Aufzeichnen von Anrufen 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	In OpenScape Business S wird bei aktiviertem Flag während der Aufzeichnung ein Hinweiston eingespielt. Standardwert: Aktiviert
Aufzeichnung von Konferenzen verfügbar	Bei aktiviertem Flag ist das Aufzeichnen von Konferenzen möglich. Standardwert: Deaktiviert
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

Parameter	Beschreibung
myPortal Einladungs-E-Mail aktivieren	Bei aktiviertem Flag erhalten UC Suite-Benutzer eine Einladungs-E-Mail zur Installation oder Aktualisierung des myPortal-Clients. Diese E-Mail wird normalerweise an alle UC Suite-Benutzer mit einer gültigen E-Mail-Adresse im Benutzerverzeichnis bei einer Neuinstallation, beim Hinzufügen oder Ändern einer E-Mail-Adresse für einen UC Suite-Benutzer im Benutzerverzeichnis oder nach einem OpenScape Business Software-Update und der Verfügbarkeit einer neuen Version des Clients gesendet. Standardwert: Aktiviert
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 (z. B. bei Systemfehlern) Standardwert: Aktiviert
Benachrichtigungen über Systemabsturz senden	Bei aktiviertem Flag erfolgt eine E-Mail-Benachrichtigung bei Systemabstürzen. Standardwert: Aktiviert
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, wenn diese jeweils eingestellten Aufbewahrungszeiten überschritten haben: <ul style="list-style-type: none"> • Nachrichten • Anrufinformationen im Anrufjournal (Anrufhistorie) • Mit myAgent aufgezeichnete Anrufe (Contact Center) • Empfangene und gesendete Faxe und E-Mails für das Contact Center • Log-Dateien Standardwert: 2.00 Stunden
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

Experten-Modus

Parameter	Beschreibung
Gespeicherte Nachrichten aufbewahren für	Aufbewahrungsdauer in Tagen für gespeicherte Sprachnachrichten Standardwert: 365
Gelöschte Nachrichten aufbewahren für	Aufbewahrungsdauer in Tagen für gelöschte Sprachnachrichten Standardwert: 30
Fax	
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
Konversation schließen nach	Aufbewahrungsdauer in Tagen für offene Gespräche im Journal. Alle nicht angenommenen Anrufe vom/zum selben Kontakt während dieses Zeitraums werden der Registerkarte "Offene Anrufe" hinzugefügt, die mit demselben Gespräch verknüpft ist. Nach Ablauf dieser Frist werden alle Anrufe in einem Gespräch als automatisch abgeschlossen markiert und aus der Registerkarte "Offene Anrufe" entfernt. Standardwert: 3 Maximalwert: 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
CC-Live-Aufzeichnung/ Rückruf/E-Mail/Fax-Anrufe aufbewahren für	Aufbewahrungsdauer in Tagen für alle Kommunikationsdaten im Zusammenhang mit Anrufen, wie Rückrufnachrichten, live aufgezeichnete Anrufe, Faxanrufe und E-Mails. Standardwert: 30
Wartung der Protokolldateien	

Parameter	Beschreibung
Protokollinformationen aufbewahren für	Aufbewahrungsdauer in Tagen für Protokolldateien Standardwert: 10
Sofortnachricht	
Sofortnachrichten aufbewahren für	Aufbewahrungsdauer in Tagen für Sofortnachrichten Standardwert: 30
Berichte	
Kennwort zurücksetzen	Zurücksetzen des myReports-Administrator-Kennworts auf das Standardkennwort
VoiceMail	
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: Vollständig
VoiceMail-Modus: Vollständig	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
Aufforderung "Bitte hinterlassen Sie eine Nachricht nach dem Ton" überspringen	Wenn dieses Flag aktiviert ist, wird die Aufforderung "Bitte hinterlassen Sie eine Nachricht nach dem Ton" übersprungen. Standardwert: Deaktiviert
Contact Card Mapping	

Experten-Modus

Parameter	Beschreibung
Microsoft: Verfügbar (grün)	Der UC-Anwesenheitsstatus dieser Zeile ist dem Outlook-Status Verfügbar (Grün) zugeordnet.
Microsoft: Nicht bei der Arbeit (gelb)	Der UC-Anwesenheitsstatus dieser Zeile ist dem Outlook-Status Nicht bei der Arbeit (Gelb) zugeordnet.
Microsoft: Beschäftigt (rot)	Der UC-Anwesenheitsstatus dieser Zeile ist dem Outlook-Status Beschäftigt (Rot) zugeordnet.
Microsoft: Außer Betrieb (grau)	Der UC-Anwesenheitsstatus dieser Zeile ist dem Outlook-Status Außer Betrieb (Grau) zugeordnet.

27.4.4.14 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)
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.
Abkürzungstasten	Aktivierung und Einrichtung von Tastaturkombination für den Zugriff auf verschiedene, häufig verwendete Funktionen über die Tastatur. Das Schlosssymbol legt fest, ob der Benutzer diese Einstellungen selbst ändern kann.

Parameter	Beschreibung
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.
Benachrichtigungen über entgangene Anrufe	Benachrichtigungsservice für entgangene Anrufe.
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.
Favoriten	
Favoriten	Favoritengruppen mit einer Liste von Kontakten, die dem Benutzer zugewiesen werden können.

Experten-Modus

Parameterbeschreibung der Registerkarten:

- **Benutzer zuordnen**

Parameter	Beschreibung
Zugewiesene Benutzer	Benutzer, für welche das Profil gelten soll
Verfügbare Benutzer	Benutzer, für die das Profil gelten soll

Parameterbeschreibung der Registerkarten:

- **Entfernen**

Parameter	Beschreibung
Name	Name des Profils (freie Eingabe)
Benutzer	Benutzer, für welche das Profil gelten soll

27.4.4.15 OpenScape Business, UC Suite > Faxkopfzeilen

Parameterbeschreibung der Registerkarten:

- **Bearbeiten**
- **Hinzufügen**
- **Entfernen**

Parameter	Beschreibung
Name der Vorlage / Name	Name der Kopfzeile (muss eindeutig sein).
Text	Platzhalter für Datum/Uhrzeit, Firmenname, Benutzername, Firmen-Rufnr., Seitennummer sowie Anzahl der Seiten können eingefügt werden.

27.4.4.16 OpenScape Business UC Suite > Skin-Einstellungen

Parameterbeschreibung der Registerkarten:

- **Skin-Einstellungen**

Parameter	Beschreibung
Skin	
Skin: Unify Standard	Das Standard-Skin wird auf die WBM-Oberfläche angewendet
Skin: Unify Dark	Das dunkle Skin wird auf die WBM-Oberfläche angewendet

27.4.5 Web Services

Unter **Web Services** sind die Funktionen für die Konfiguration der Web-Schnittstellen zusammengefasst, wie z . B. zu Web Collaboration.

27.4.5.1 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).

Parameterbeschreibung der Registerkarten:

- **Web Collaboration Server**

Parameter	Beschreibung
Server Typ	Auswahl des Web Collaboration Servers.
Server-Typ: Öffentlicher 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 dafür der TCP-Port 5100 verwendet.
Server-Typ: Öffentlicher Server (Demomodus/ Evaluierungsmodus)	Die Web Collaboration kann 5 min lang getestet werden. Dafür ist keine Eingabe von IP-Adresse, Lizenznummer und Passwort nötig.
Server-Typ: Benutzerdefinierter 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 dafür 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: <code>http://<Webcollaboration Server IP Adresse>:5004/OscInterface</code> <code>https://<Webcollaboration Server IP Adresse>:5100/XMLRPSecure</code>
Lizenznummer	Lizenznummer für die gesicherte Verbindung zum Web Collaboration Server.
Kennwort	Passwort für die gesicherte Verbindung zum Web Collaboration Server.

27.4.6 Open Directory Service

Unter **Open Directory Service** sind die Funktionen für die Konfiguration von Open Directory Service zusammengefasst.

27.4.6.1 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.

27.4.6.2 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.
Kurzwahlliste	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

27.4.6.3 Open Directory Service > Datenquellen > LXV3

Parameter	Beschreibung
Kurzwahlliste	Zentrale Kurzwahlnummern. Das Verzeichnis ist Open Directory Service fest zugeordnet und kann nicht gelöscht oder geändert werden.

27.4.6.4 Open Directory Service > Datenquellen > LXV3

Parameter	Beschreibung
Überblick über die konfigurierten Datenquellen	Eine LDAP-Ausgabebezuordnung 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-Ausgabebezuordnung 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 zudem weitere LDAP-Ausgabebezuordnungen konfigurieren.
Hinzufügen	Weitere Ausgabebezuordnungen hinzufügen. Über den Parameter dc im LDAP-Login können LDAP-Clients auf eine bestimmte LDAP-Ausgabebezuordnung zugreifen, z.B.: dc=web.

27.4.6.5 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

27.4.6.6 OpenStage Gate View

Unter **OpenStage Gate View** kann OpenStage Gate View aktiviert oder deaktiviert werden und die OpenStage Gate View Server-Software gestartet werden.

27.4.7 OpenStage Gate View

Parameter	Beschreibung
Aktivieren	OpenStage Gate View aktivieren.
Deaktivieren	OpenStage Gate View deaktivieren.
Login	Aufrufen der OpenStage Gate View Server-Software.

27.4.8 Application Launcher

Unter **Application Launcher** sind die Funktionen für die Konfiguration von Application Launcher zusammengefasst.

27.4.8.1 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

27.5 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 aktiviert	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.

Parameter	Beschreibung
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)

Dienste

- 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

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.
Calling Line Identification Presentation (CLIP)	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.
Calling Line Identification Restriction (CLIR)	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).

Thema	Erklärung
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 Anrufwefterschaltung leitet Anrufe bei Besetzt an jeden beliebigen, aber erreichbaren Telefonanschluss weiter. Die Anrufwefterschaltung wird in der Vermittlungsstelle durchgeführt. Beide Nutzkanäle bleiben dadurch frei.
Direkte Anrufumleitung (CFU = Call Forwarding Unconditional)	Diese Anrufwefterschaltung leitet Anrufe sofort an jeden beliebigen, aber erreichbaren Telefonanschluss weiter. Die Anrufwefterschaltung wird in der Vermittlungsstelle durchgeführt. Beide Nutzkanäle bleiben dadurch frei.
Verzögerte Anrufumleitung (CFNR = Call Forwarding No Reply)	Diese Anrufwefterschaltung leitet Anrufe nach 20 Sekunden (bei nicht Erreichen) an jeden beliebigen, aber erreichbaren Telefonanschluss weiter. Die Anrufwefterschaltung wird in der Vermittlungsstelle durchgeführt. Beide Nutzkanäle bleiben dadurch frei.

Thema	Erklärung
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 OpenScope 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.

Eine aktuelle und vollständige Liste aller verwendeten Ports von OpenScope Business finden Sie in der „Interface Management Database“ (IFMD), die über das Partnerportal von Unify (<https://unify.com/en/partners/partner-portal>) zugänglich ist.

Anmerkung: Die in der folgenden Liste mit „O“ gekennzeichneten Ports sind optional, d. h. sie sind in der Firewall nicht permanent geöffnet.

Anhang

Beschreibung	TCP	UDP	Portnummer	OpenScope Business X	UC Booster Card	OpenScope 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
CLS	X		7780 7790	O		O	
Communication Client-Installationsprogramm	X		8101	X	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	
HFA	X		4060	X		X	
HFA Secure	X		4061	X		X	
Instant Messaging (http)	X		8101	X	X	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
xNAT 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
xOpenfire Admin (https)	X		9091		X	X	X
OpenScape Business Auto Update Service (http)	X		8101	X	X	X	X
OpenScape Business Multisite	X		8778		X	X	X
OpenScape Business myReports (http)	X		8101		X	X	X
OpenScape Business Status Server	X		8808	X		X	X
OpenScape Business Benutzerportal	X	X	8779		X	X	X
Postgres	X		5432	X	X	X	X
RTP (eingebettet)		X	29100-30530	X	X	X	X
RTP (Server)		X	29100-30888	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	
VSL	X		8770-8780		X	X	X
Webadmin for Clients	X		8803	X	X	X	X
Webbased Clients							
Webbased Clients (http)	X		8801	X	X	X	X
Webbased Clients (https)	X		8802	X	X	X	X

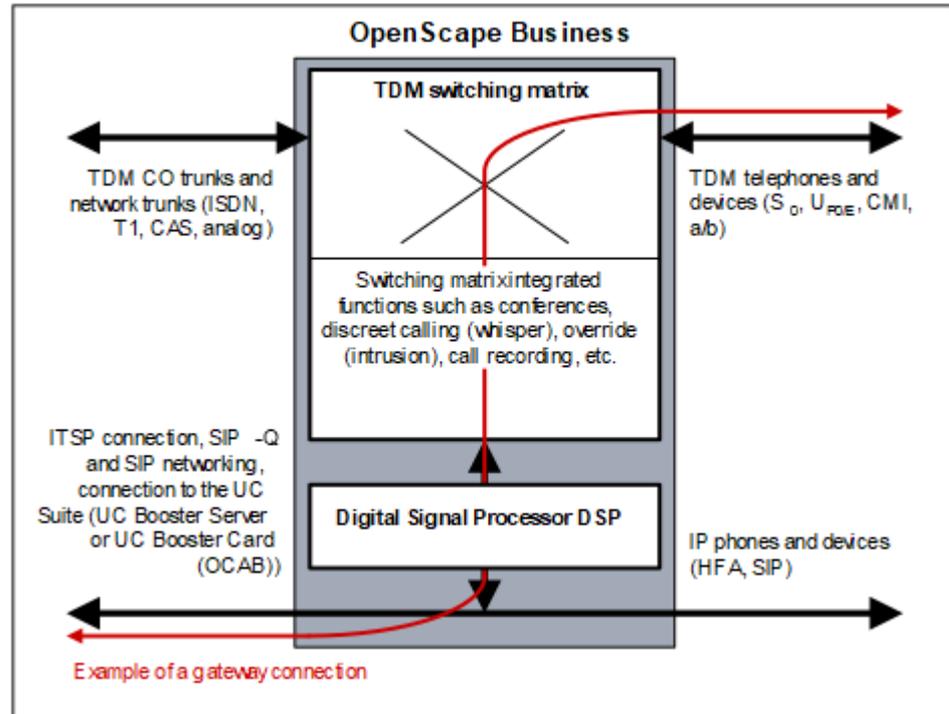
Anmerkung: Aus Sicherheitsgründen wird empfohlen für die Webbased Clients ausschließlich https zu verwenden und ein Port Forwarding von extern TCP/443 nach intern TCP/8802 einzurichten.

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 OpenScope 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.

Im Fall von UC-Suite Konferenzen und IP-Telefonen kann ein Kommunikationssystem OpenScope Business X3/X5/X8 bis zu acht DSP-Kanäle umfassen. Standardmäßig werden drei DSP-Kanäle für die 3 Standard-Codexs der Wartemusik zugewiesen. Diese Zahl kann verringert werden, wenn Sie weniger Codexs für die Wartemusik verwenden. Zusätzlich sind zwei DSP-Kanäle für die Konfiguration der Signaling and Payload Encryption (SPE) reserviert. Der Rest der DSP-Kanäle kann den IP-Telefonen zugewiesen werden (ein DSP-Kanal pro IP-Telefon). Wenn die vorhandenen DSP-Kanäle erschöpft sind, kann die Anzahl der DSP-Kanäle durch die Verwendung der entsprechenden

OCCB-Karten (OCCB1 oder OCCB3, wie zuvor angegeben) erhöht werden.

Tipp: Weitere Angaben zu den maximal zur Verfügung stehenden DSP-Kanälen der Mainboards und der OCCB-Submodule finden Sie unter [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.	<p>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.</p> <p>INFO: Die Option Ausschließlich G.711 verwenden kann durch einen Administrator mit dem Profil Experte im Experten-Modus (Telephonie > Sprachgateway > Codec-Parameter) aktiviert werden.</p>

Die folgende Tabelle liefert Orientierungswerte, ob und welches OCCB-Submodul einzusetzen ist.

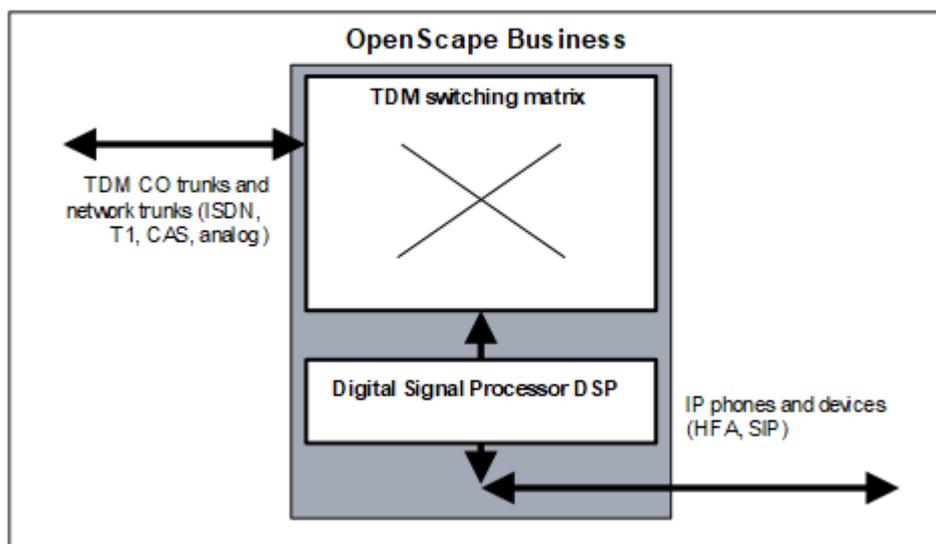
Anhang

Summe der TDM-Kanäle: Amts- und Vernetzungsleitun (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?	Bemerkungen
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	Unabhängig von den TDM-Kanälen. Smart VM und Systemkonferenzen in Kombination mit IP-Telefonen und IP-Geräten benötigen bis zu 40 DSP-Ressourcen gleichzeitig.
			> 100	OCCB3	Unabhängig von den TDM-Kanälen. Smart VM und Systemkonferenzen in Kombination mit IP-Telefonen und IP-Geräten benötigen bis zu 120 DSP-Ressourcen gleichzeitig.
	> 0	bis 8		Kein OCCB-Submodul	
	> 0	9 bis 100		OCCB1	Bis 40 gleichzeitig

Summe der TDM-Kanäle: Amts- und Vernetzungsleitun (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/Er} , CMI, a/b)	Summe der IP-Telefone und IP-Geräte (HFA, SIP)	Welches OCCB-Submodul?	Bemerkungen
	> 0	> 100		OCCB3	Bis 120 gleichzeitig
> 0	bis 8			Kein OCCB-Submodul	Kombination ist im wesentlichen bei SIP-Q und UC Suite relevant.
> 0	9 bis 40			OCCB1	Kombination ist im wesentlichen bei SIP-Q und UC Suite relevant.
> 0	> 40			OCCB3	Kombination ist im wesentlichen bei SIP-Q und UC Suite relevant.

Die folgenden Beispiele liefern Orientierungswerte, ob und welches OCCB-Submodul einzusetzen ist.

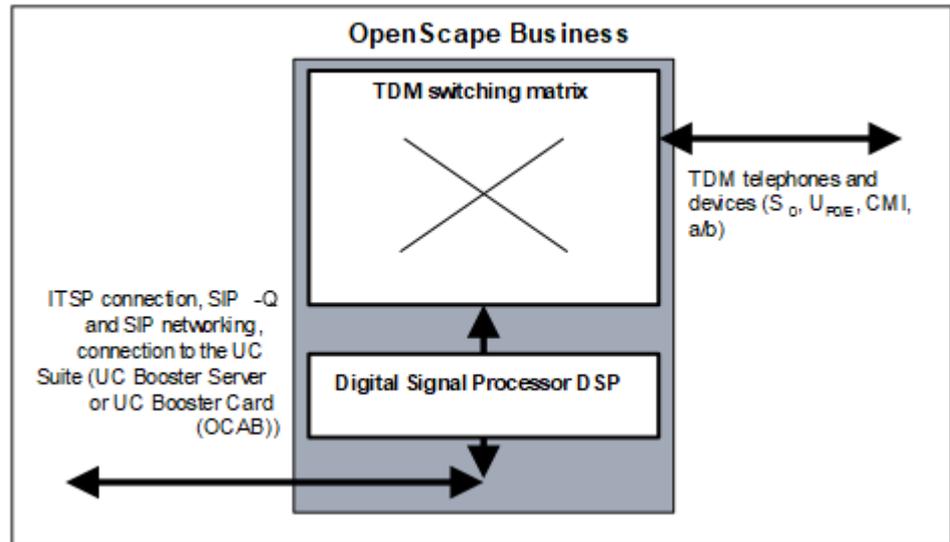
Beispiel 1: OpenScape Business mit TDM-Amtsleitungen und IP-Telefonen und -Geräten



Wenn	Dann
OpenScape Business mit: <ul style="list-style-type: none"> • 1 x TDM-Amt (ISDN) • 20 x IP-Telefon (HFA, SIP) 	Die DSP-Kanäle des Mainboards werden genutzt. Kein OCCB-Submodul erforderlich.
OpenScape Business mit: <ul style="list-style-type: none"> • 1 x TDM-Amt (ISDN) • 100 x IP-Telefon (HFA, SIP) 	Submodul OCCB1 ist erforderlich. Alternativ kann Submodul OCCB3 eingesetzt werden.
OpenScape Business mit: <ul style="list-style-type: none"> • 2 x TDM-Amt (ISDN) • 100 x IP-Telefon (HFA, SIP) 	Submodul OCCB3 ist erforderlich.
OpenScape Business mit: <ul style="list-style-type: none"> • 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.

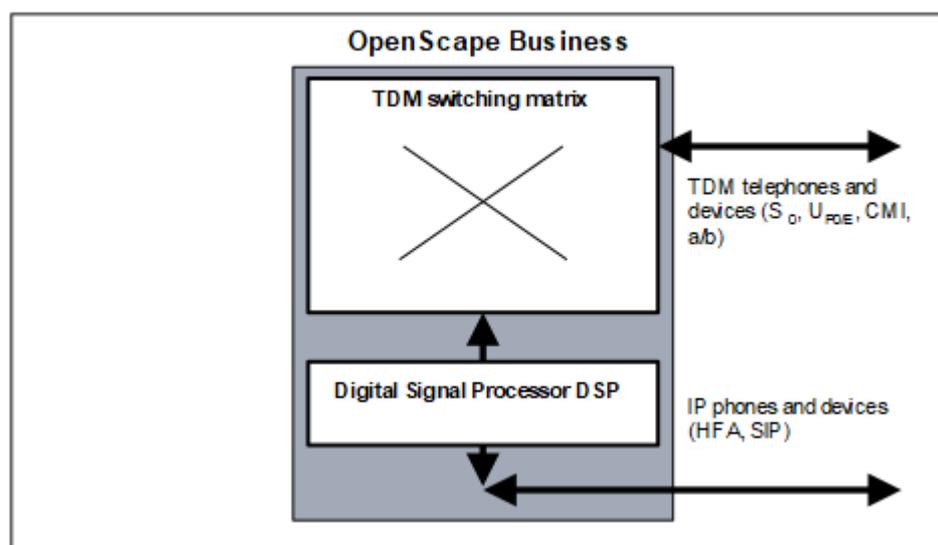
Beispiel 2: OpenScape Business mit ITSP-Verbindungen und TDM-Telefonen und -Geräten



Wenn	Dann
OpenScape Business mit: <ul style="list-style-type: none"> • 6 x ITSP-Anschaltung (6 B-Kanäle) • 20 x TDM-Telefon (S_0, $U_{P0/E}$, CMI, a/b) 	Die DSP-Kanäle des Mainboards werden genutzt. Kein OCCB-Submodul erforderlich.
OpenScape Business mit: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 6 x TDM-Telefon (S_0, $U_{P0/E}$, CMI, a/b) • 6 x IP-Telefon (HFA, SIP) 	Die DSP-Kanäle des Mainboards werden genutzt. Kein OCCB-Submodul erforderlich.
OpenScape Business mit: <ul style="list-style-type: none"> • 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.

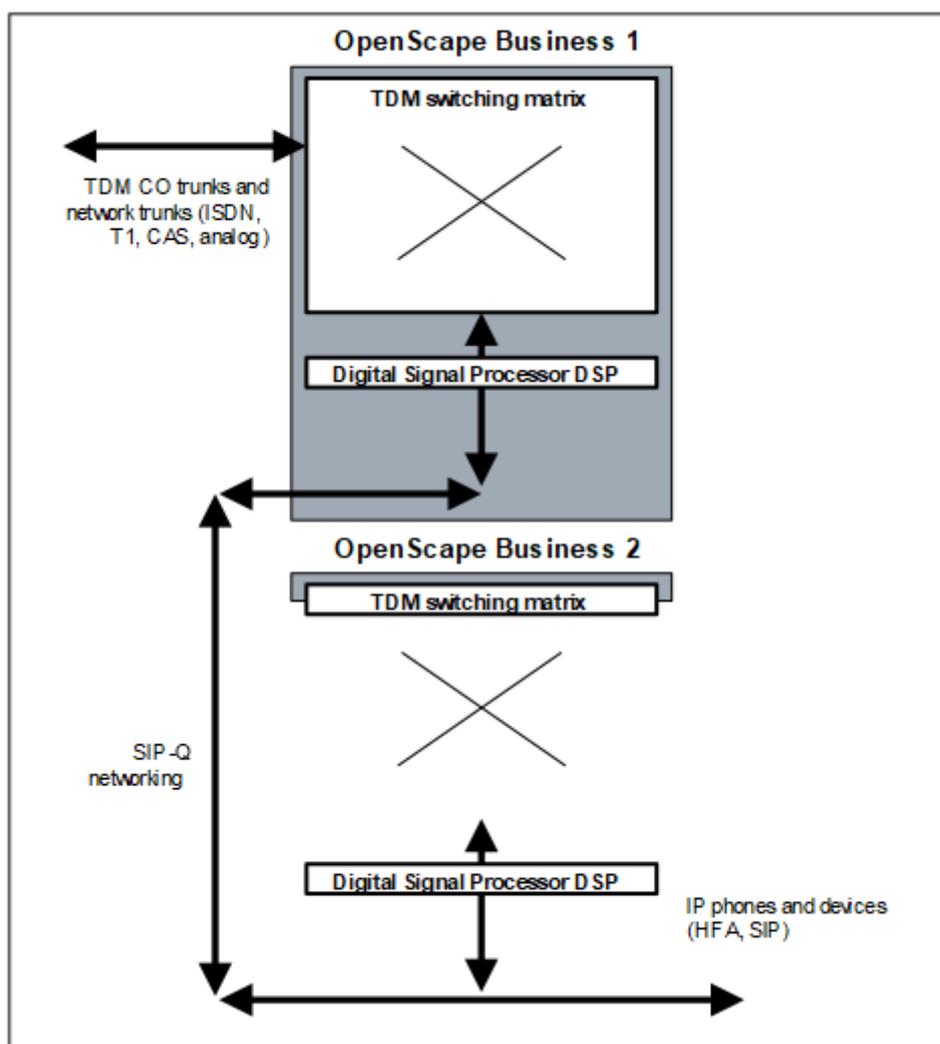
Beispiel 4: SIP-Q-Vernetzung OpenScape Business

Anmerkung: Dieses Beispiel beschreibt die Anforderungen eines vernetzten zweiten OpenScape Business Systems. Verbindungen im ersten System werden hier aus Gründen der Einfachheit nicht dargestellt. Allerdings sind auch die Anforderungen des ersten Systems, wie in den Beispielen 1, 2 und 3 angegeben, zu berücksichtigen.

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: <ul style="list-style-type: none"> • 1 x TDM-Amt (ISDN) OpenScape Business 2 mit: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 2 x TDM-Amt (ISDN) OpenScape Business 2 mit: <ul style="list-style-type: none"> • 100 x IP-Telefon (HFA, SIP) 	Submodul OCCB3 ist in OpenScape Business 1 erforderlich. Kein OCCB-Submodul in OpenScape Business 2 erforderlich.

Wenn	Dann
OpenScape Business 1 mit: • 4 x TDM-Amt (ISDN)	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.
OpenScape Business 2 mit: • 500 x IP-Telefon (HFA, SIP)	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.

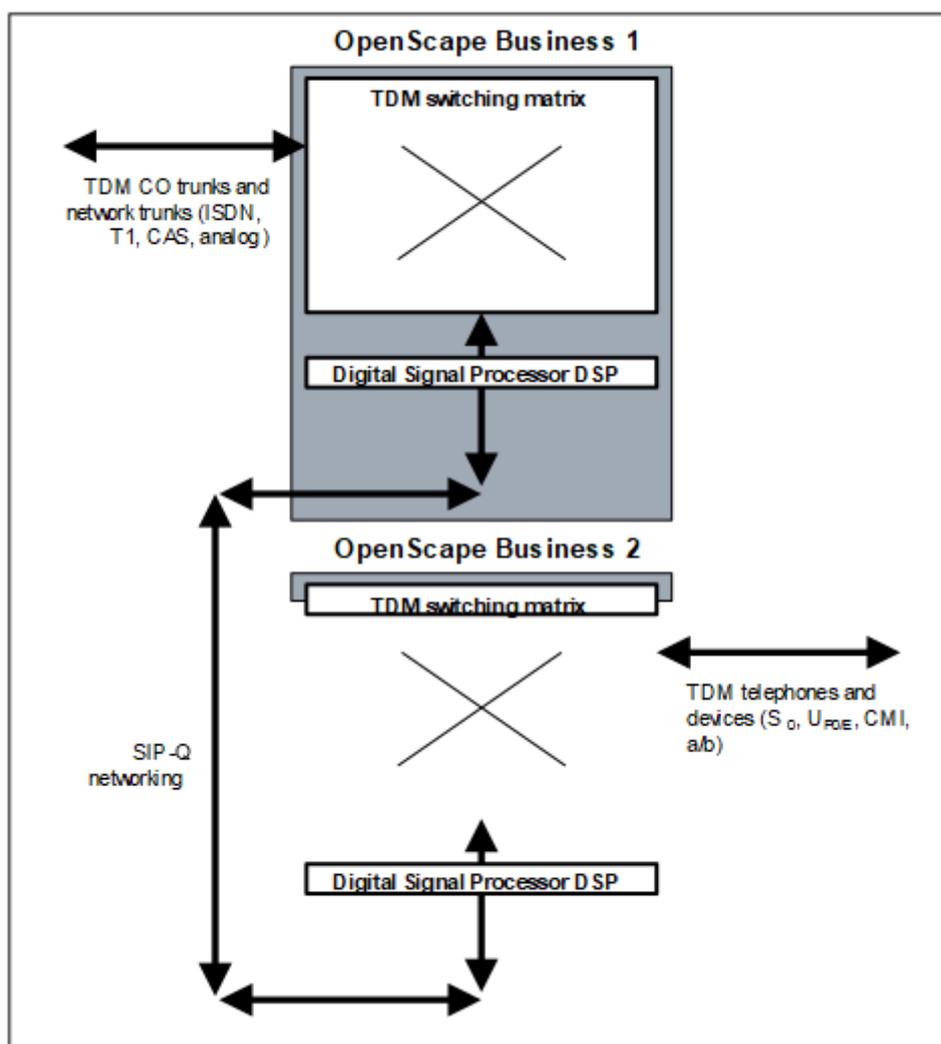
Beispiel 5: SIP-Q-Vernetzung OpenScape Business

Anmerkung: Dieses Beispiel beschreibt die Anforderungen eines vernetzten zweiten OpenScape Business Systems. Verbindungen im ersten System werden hier aus Gründen der Einfachheit nicht dargestellt. Allerdings sind auch die Anforderungen des ersten Systems, wie in den Beispielen 1, 2 und 3 angegeben, zu berücksichtigen.

Kommunikationssystem OpenScape Business 1 fungiert als Gateway zum TDM-Amt.

Ausschließlich am Kommunikationssystem OpenScape Business 2 sind TDM-Telefone (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: <ul style="list-style-type: none"> • 1 x TDM-Amt (ISDN) OpenScape Business 2 mit: <ul style="list-style-type: none"> • 100 x TDM-Telefon (S₀, 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: <ul style="list-style-type: none"> • 2 x TDM-Amt (ISDN) OpenScape Business 2 mit: <ul style="list-style-type: none"> • 100 x TDM-Telefon (S₀, 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 (S₀, U_{P0/E}, CMI, a/b) ausgestattet werden, sind dafür zusätzliche DSP-Kanäle zu berücksichtigen.

Beispiel 6: OpenScape Business mit IP-Telefonen und -Geräten

Anmerkung: Dieses Beispiel beschreibt die Anforderungen eines vernetzten zweiten OpenScape Business Systems. Verbindungen im ersten System werden hier aus Gründen der Einfachheit nicht dargestellt. Allerdings sind auch die Anforderungen des ersten Systems, wie in den Beispielen 1, 2 und 3 angegeben, zu berücksichtigen.

Wenn	Dann
OpenScape Business X3/X5/X8 mit: <ul style="list-style-type: none"> • 7 x IP-Telefon (HFA, SIP) 	Die DSP-Kanäle des Mainboards werden genutzt. Kein OCCB-Submodul erforderlich.
OpenScape Business: <ul style="list-style-type: none"> • 30 x IP-Telefon (HFA, SIP) 	Submodul OCCB1 ist erforderlich. Alternativ kann Submodul OCCB3 eingesetzt werden.
OpenScape Business mit: <ul style="list-style-type: none"> • 100 x IP-Telefon (HFA, SIP) 	Submodul OCCB3 ist erforderlich.

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)

Das 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.

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 seiner 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 Standard-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 herstellereigene 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 widerrufenen 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 Zugriffsmöglichkeiten 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 Methode 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 Rechnernetzwerken 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 Mobiltelefonen. 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, Leitweglenkung)

Mit Hilfe von LCR (Least Cost Routing, Leitweglenkung) 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.

DTMF (Dual Tone Multifrequency)

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 Virens scanner 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-Protokoll (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 höchstmögliche 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 sicher 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 Dateiübertragungsschnittstellen 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 Protocol)

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 Rechner 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).

Anrufverteilung (UCD Uniform Call Distribution)

UCD ermöglicht eine gleichmäßige 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, der deutlich höhere Datenübertragungsraten (384 kbit/s bis 7,2 Mbit/s) ermöglicht als der Mobilfunkstandard der zweiten Generation oder der GSM-Standard.

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 kürzere Entfernungen symmetrische oder asymmetrische Datenströme mit hoher Geschwindigkeit zu übertragen sind. VDSL stellt eine Alternative zu ADSL und SDSL dar, aber mit höheren 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.

Index

Sonderzeichen

<\$nopage>Central License Server (siehe Lizenzserver) [179](#)
 <\$nopage>Medium, Backup (siehe Backup-Medium) [706](#)
 <\$nopage>Restore (siehe Wiederherstellen) [708](#)
 <\$nopage>UCD (Uniform Call Distribution) (siehe Anrufverteilung) [401](#)

A

Ablauf der Lizenzierung [172](#)
 Abteilungen [302](#)
 Abteilungen, Experten-Modus [1145](#)
 Abwesenheitstexte [359](#)
 Abwurf/VPL/Hotline, Experten-Modus [939](#)
 Active Directory Integration Service, Experten-Modus [1138](#)
 Active Directory Service [679](#)
 Ad-hoc-Konferenz [262](#), [310](#)
 Admin-Protokoll [579](#)
 Admin-Protokoll-Daten, Experten-Modus [911](#)
 Konfiguration, Experten-Modus [911](#)
 Admin-Protokoll-Daten, Experten-Modus [911](#)
 Admin-Protokoll, Experten-Modus [911](#)
 AF/EF-Codepunkte [214](#)
 Aktionen
 Automatische Aktionen, Experten-Modus [914](#), [915](#)
 Manuelle Aktionen, Experten-Modus [912](#)
 Aktionen, Experten-Modus [912](#)
 Aktive Dienste, Experten-Modus [974](#)
 Aktive Regeln, Experten-Modus [983](#)
 Aktive Tunnel, Experten-Modus [975](#)
 Aktive Zertifikate, Experten-Modus [971](#)
 Aktivierung, Software (siehe Software-Aktivierung) [708](#)
 Aktualisierung, Software (siehe Software-Aktualisierung) [708](#)
 Aktualisierungszeit der DNS Namen, Experten-Modus [949](#)
 Alarm-Signalisierungs, Experten-Modus [906](#)
 Alle Leases, Experten-Modus [1003](#)
 alternativer Arbeitsplatz [287](#)
 Amtsberechtigung [410](#)
 Analoge Teilnehmer, Experten-Modus [1052](#)
 Analoges Telefon [222](#)
 Anklopfen/Rufeinblendung [357](#)
 Announcement Player, Experten-Modus [957](#)
 Anruf
 entgangen [303](#)
 geplant [303](#)
 Anrufbeantworter [222](#)

Anrufbeantworter-Gruppe (siehe Sprachbox-Gruppe) [398](#)
 Anrufe abweisen [354](#)
 Anrufschutz [355](#)
 Anrufübernahme von Sprachbox [318](#)
 Anrufübernahme, Experten-Modus [1094](#)
 Anrufübernahmegruppe [371](#)
 Anrufübernahme außerhalb einer AUN-Gruppe [372](#)
 Anrufübernahme von Wiederanrufen [371](#)
 Aufmerksamkeitston [371](#)
 Namensanzeige des Anrufers [371](#)
 Rufnummernanzeige des Anrufers [371](#)
 SIP-Telefone [371](#)
 Anrufumleitung [349](#)
 regelbasiert [289](#)
 statusbezogen [288](#)
 Anrufverteilung [401](#), [401](#)
 AICC (Automatic Incoming Call Connection) [405](#)
 Ansagen [408](#)
 Konfiguration [401](#)
 Nachbearbeitungszeit [404](#)
 Nachtschaltung [407](#)
 Priorität externer Anrufe [404](#)
 Priorität interner Anrufe [404](#)
 Teilnehmerzustand [402](#)
 Übergabe an UCD-Gruppe [408](#)
 Überlauf [406](#)
 UCD-Agent [402](#)
 UCD-Anrufe automatisch annehmen [405](#)
 UCD-Anrufe über analoge Leitungen auslösen [409](#)
 UCD-Gruppe [401](#)
 Wartemusik (Music On Hold MOH) [408](#)
 Warteschlange [406](#)
 Ansagen bei Anrufverteilung [408](#)
 Ansagen für Sprachbox [318](#)
 Ansagen und Wartemusik, Experten-Modus [1122](#)
 Anschaltungen
 Ansagen/Wartemusik, Experten-Modus [1122](#)
 SmartVM, Experten-Modus [1124](#)
 Türsprechstelle, Experten-Modus [1123](#)
 Anschaltungen, Experten-Modus [1081](#), [1122](#)
 Anschlussbereich
 OpenScape Business S [42](#)
 OpenScape Business UC Booster Server [42](#)
 Anwesenheit (UC Smart) [251](#)
 Anwesenheitsstatus [271](#)
 Anrufumleitung [288](#)
 Anwesenheitsstatus (UC Smart) [251](#)
 Anwesenheitsstatus (UC Suite) [284](#)
 Application Firewall, Experten-Modus [962](#)
 Application Launcher
 Profil für Konfigurationsdaten [682](#)

Application Launcher [681](#), [1176](#)
 Application Launcher, Experten-Modus [1175](#), [1176](#)
 Applikat.-Diagnose, Experten-Modus [916](#)
 Applikationen, Experten-Modus [1137](#), [1176](#)
 Applikationsauswahl [1137](#)
 Applikationsdiagnose
 Entwickler-Einstellungen, Experten-Modus [916](#),
 [916](#)
 Mainboard, Experten-Modus [916](#)
 Applikationsgesteuerte Konferenz [262](#), [307](#)
 ARP-Protokoll, Experten-Modus [917](#)
 Audio-Codec [213](#)
 Audio-Datei [701](#), [703](#)
 Aufschalten [358](#)
 Aufzeichnen [306](#)
 Ausbaugrenzen [832](#)
 Ausnahme
 regelbasierte Anrufumleitung [289](#)
 Authentifizierung
 Konferenzteilnehmer [262](#)
 AutoAttendant [317](#)
 Automatische Aktion [719](#)
 DLS Notification [719](#)
 Garbage Collection [719](#)
 Automatische Nachtschaltung, Experten-Modus
[1121](#)
 automatische Updates [279](#)
 Automatischer Rückruf [356](#)

B

Backup [705](#)
 Backup-Medium [705](#), [706](#)
 Backup-Set [705](#), [706](#), [706](#)
 Backup-Set für Diagnosezwecke [749](#)
 Backup-Verzeichnis [706](#)
 Bandbreiten im LAN [592](#)
 Basic-MULAP [392](#)
 Rufart [393](#)
 Basisstationen, Experten-Modus [886](#), [886](#), [1055](#),
[1085](#)
 Baugruppen-Zustand, Experten-Modus [889](#)
 Bedingung
 regelbasierte Anrufumleitung [289](#)
 Benachrichtigung
 Faxnachricht [324](#)
 Sprachnachricht [269](#), [324](#)
 Benachrichtigungsdienst [269](#), [324](#)
 Benutzer der UC Suite [279](#)
 Benutzer-Profile der UC Suite [282](#)
 Benutzerschaltflächen [483](#)
 Layout [483](#)
 Benutzerverzeichnis, Experten-Modus [1142](#)
 Berechtigungen, Experten-Modus [1020](#), [1114](#)
 Berechtigungsklassen
 Automatische Nachtschaltung, Experten-Modus
[1121](#)

Erlaubnislisten, Experten-Modus [1117](#)
 Nacht: Berechtigungsgruppen, Experten-Modus
[1116](#)
 Nachtschaltung, Experten-Modus [1119](#)
 Sondertage, Experten-Modus [1121](#)
 Tag: Berechtigungsgruppen, Experten-Modus
[1115](#)
 Teilnehmer, Experten-Modus [1115](#)
 VBZ Gruppenzuordnung, Experten-Modus [1119](#)
 VBZ Matrix, Experten-Modus [1120](#)
 Verbotslisten, Experten-Modus [1117](#), [1118](#)
 Bestimmungsgemäßer Gebrauch der
 Kommunikationssysteme und Server [40](#)
 Betriebsbedingungen (klimatisch, mechanisch)
 OpenScope Business S [48](#)
 OpenScope Business UC Booster Server [48](#)
 OpenScope Business X3, X5, X8 [47](#)
 Blitzschutzanforderungen [43](#)
 Blockwahl [328](#)
 Branding, Experten-Modus [881](#)
 Brandschutzanforderungen [43](#)
 Breitbandverbindung [192](#)

C

Call Supervision, Experten-Modus [897](#)
 CallMe [287](#)
 CallMe-Dienst [287](#)
 Carrier Select Override [422](#)
 CCV-Objekte [467](#), [505](#)
 CDP (Certificate Distribution Point) [578](#)
 CE-Kennzeichnung [44](#)
 CE-Konformität [46](#)
 Chef-Funktion (siehe Chef/Sekretär-Konfiguration)
[386](#)
 Chef-MULAP [394](#)
 Rufart [396](#)
 SIP-Telefone [396](#)
 Chef/Sekretär (siehe Chef/Sekretär-Konfiguration)
[386](#)
 Chef/Sekretär-Konfiguration [386](#)
 Faxbox [389](#)
 Rufart [389](#)
 SIP-Telefone [389](#)
 Client (UC Smart) [232](#)
 Client (UC Suite) [271](#)
 Client Logs [751](#)
 Clients, Hardware- und Softwarevoraussetzungen
[274](#), [479](#), [490](#), [493](#)
 CLIP - Rufnummernübermittlung des Anrufers [336](#)
 CLIP no screening [338](#)
 Clipboard-Wahl [305](#)
 CLIR - Rufnummernunterdrückung des Anrufers [337](#)
 CMD (CSTA Message Dispatcher) [1176](#)
 Codec-Parameter, Experten-Modus [1024](#)
 Codeschloss individuell [418](#)

COLP - Rufnummernübermittlung des Angerufenen [338](#)
 COLR - Rufnummernunterdrückung des Angerufenen [338](#)
 Communities, Experten-Modus [909](#)
 Contact Center [467](#), [467](#), [467](#), [467](#), [487](#), [504](#), [505](#), [505](#), [505](#)
 Agent [496](#)
 Agentenrückruf [515](#)
 Anzeige der Warteschlangendetails [514](#)
 Bedingungen für den Betrieb [523](#)
 Berechtigungs-Level eines Agenten [496](#), [496](#)
 Berichte [528](#)
 bevorzugte Agenten [498](#)
 Clients [488](#)
 Einsatz von DECT-Telefonen [526](#)
 Einschränkungen von System-Leistungsmerkmalen [525](#)
 myAgent [488](#)
 myReports [491](#)
 myReports Benutzerrollen [492](#)
 Nachbearbeitung [513](#)
 Nachbearbeitungsgründe [513](#)
 Pause [498](#)
 Rückfalllösung (Fallback-Lösung) [516](#)
 Servicegrad [514](#)
 VIP-Anruferpriorität [515](#)
 VIP-Rufliste [516](#)
 vordefinierte Berichtsvorlagen [529](#)
 Vorgehensweise bei der Konfiguration [522](#)
 Wandanzeige/Wallboard [514](#)
 Warteschlange [503](#)
 Contact Center, Experten-Modus [1150](#)
 Contact Center:Beispiel für eine Contact-Center-Konfiguration [520](#)
 Contact Center:Konfiguration [520](#)
 Cordless
 Basisstationen, Experten-Modus [1085](#)
 Multi-SLC, Experten-Modus [1084](#)
 SLC, Experten-Modus [1083](#)
 Systemweit, Experten-Modus [1081](#)
 Cordless-Lösung
 Systemausbau [546](#)
 Corporate Network [428](#)
 Cover Page Editor [323](#)
 CRL (Certificate Revocation Lists) [573](#), [578](#)
 CSP (CSTA Service Provider) [1177](#)
 CSTA Message Dispatcher (CMD) [1176](#)
 CSTA Service Provider (CSP) [1177](#)
 CSTA-Protokoll [661](#)
 CSV-Datei [211](#)

D

Darstellungskonventionen [29](#)
 Datei-Upload, Experten-Modus [1161](#)
 Datenschutz [45](#), [528](#)

Datensicherheit [45](#)
 Datensicherung (siehe Sichern) [705](#)
 Datum und Uhrzeit, Experten-Modus [951](#)
 Dauerhaft [313](#)
 DECT Teilnehmer, Experten-Modus [1056](#)
 DECT-Telefone [69](#)
 Default Router [188](#)
 Default Router, Experten-Modus [1006](#), [1008](#)
 Deployment- und Licensing-Client (DLSC), Experten-Modus [963](#)
 DeskSharing [542](#)
 Desktop-Wahl [272](#), [305](#)
 Device-Statistik, Experten-Modus [1132](#)
 Devices, Experten-Modus [1128](#)
 DHCP Modus, Experten-Modus [998](#)
 Diagnose Log [748](#)
 Diagnose Logs, Experten-Modus [906](#), [912](#)
 Diagnose-Protokoll [736](#)
 Diagnosedaten [736](#)
 Dial In Control Server [428](#)
 Digitale Prüfschleife [740](#)
 Digitale Prüfschleife, Experten-Modus [893](#)
 Digitale Signatur [571](#)
 Direktansprechen [334](#)
 Direktansprechen für Gruppen [399](#)
 Direktansprechschutz für Teilnehmer [334](#)
 Direktantworten [334](#)
 Direktruftaste [333](#)
 DISA, Experten-Modus [938](#)
 Diskretes Ansprechen) [345](#)
 Display, Experten-Modus [934](#)
 DLI-Wartung, Experten-Modus [914](#)
 DLS Notification, Experten-Modus [915](#)
 DLSC CA -Zertifikat, Experten-Modus [965](#)
 DLSC Client-Zertifikat, Experten-Modus [964](#)
 DNS-Name [196](#)
 DNS-Server [188](#)
 DNS-Server, Experten-Modus [1007](#)
 Download (siehe Update) [708](#)
 DSL (Digital Subscriber Line) [192](#)
 DSP-Kanäle projektieren [1186](#)
 DSS-Server [1178](#)
 DSS-Taste [333](#)
 Dual-Mode-Telefonie [540](#)
 Durchsage an Gruppe [400](#), [400](#)
 Gespräch übergeben [400](#)
 Durchwahl Rufnummern, Experten-Modus [1075](#)
 DynDNS [187](#)
 DynDNS (Dynamic Domain Name Service) [196](#)
 DynDNS Service, Experten-Modus [948](#)
 DynDNS-Service [196](#)

E

E-Mail
 Benachrichtigung [269](#), [324](#)
 Einladung zu Konferenz [262](#)

E-Mail to SMS [325](#)
 E-Mail-Einstellungen [748](#)
 E-Mail-Versand [325](#)
 E-Mail, Experten-Modus [904](#)
 E.164-Nummerierung [594](#)
 Editieren der Wahl [329](#)
 Eingehende Anrufe
 Anrufübernahme, Experten-Modus [1094](#)
 Gruppen-/Sammelanschluss, Experten-Modus [1086](#)
 Gruppen-Teilnehmer, Experten-Modus [1089](#)
 Team/Top, Experten-Modus [1091](#)
 UCD, Experten-Modus [1095](#)
 Einladung
 Konferenz [262](#)
 Einwahlnummer
 Konferenz [262](#)
 Endgerät
 Tastenprogrammierung, Experten-Modus [1080](#)
 Teilnehmer, Experten-Modus [1050](#), [1052](#), [1054](#),
 [1055](#), [1056](#), [1058](#), [1059](#), [1073](#), [1075](#), [1075](#)
 Entsorgung [41](#)
 Ereignisse
 Diagnose Logs, Experten-Modus [906](#)
 Event-Konfiguration, Experten-Modus [904](#)
 Event-Protokoll, Experten-Modus [904](#)
 Reaktionstabelle, Experten-Modus [905](#)
 Erlaubnislisten, Experten-Modus [1117](#)
 ESP-Header [567](#)
 Euro-ISDN-Leistungsmerkmale [1181](#)
 Event (Ereignis) [747](#), [747](#), [747](#), [748](#), [748](#)
 Event Viewer [740](#)
 Event-Konfiguration, Experten-Modus [904](#)
 Event-Protokoll, Experten-Modus [904](#)
 Events
 Alarm-Signalisierung, Experten-Modus [906](#)
 E-Mail, Experten-Modus [904](#)
 Events, Experten-Modus [904](#)
 EVM, Experten-Modus [1058](#)
 Experten-Modus, Experten-Modus [874](#)
 Externes Verzeichnis [293](#)
 Externes Verzeichnis (LDAP) [295](#)
 Externes Verzeichnis, Experten-Modus [1147](#)

F

FastViewer [264](#), [315](#), [315](#)
 Favoritenliste [302](#)
 Sofortnachricht [265](#)
 Favoritenliste (UC Smart) [253](#)
 Fax [318](#)
 T.38 [326](#)
 Fax Gruppe 3 [222](#)
 Fax Gruppe 4 [221](#)
 Fax Printer [272](#), [323](#)
 Faxbox [322](#)
 Faxbox-Gruppe [398](#)

Faxgruppe (siehe Faxbox-Gruppe) [399](#)
 Faxkopfzeilen, Experten-Modus [1172](#)
 Faxnachrichten [318](#), [484](#)
 Fernzugriff auf das Kommunikationssystem [759](#)
 Feste Rufweitschaltung [348](#)
 Firewall [559](#), [681](#)
 Flex Call [361](#)
 Flexible Menüs, Experten-Modus [944](#)
 FTP-Server, Experten-Modus [997](#)
 Funkstörung [44](#)
 Funktionen
 myPortal [271](#)
 myPortal for Outlook [272](#)
 myPortal Smart [234](#)
 Funktionstasten [224](#)

G

Garbage Collection, Experten-Modus [914](#)
 Gateview [1175](#)
 Gateway, Experten-Modus [947](#)
 Gebühren Ausgabe, Experten-Modus [953](#)
 Gebühren Faktoren, Experten-Modus [955](#)
 Gebühren Projekt Kennzahlen, Experten-Modus [957](#)
 Geplante Konferenz [262](#), [311](#), [311](#)
 Gigaset-Telefone [69](#)
 Globale Parameter, Experten-Modus [998](#)
 Grundeinstellungen [919](#)
 Datum und Uhrzeit, Experten-Modus [951](#), [951](#),
 [952](#)
 DynDNS, Experten-Modus [948](#), [949](#)
 Gateway, Experten-Modus [946](#), [947](#)
 Gebühren, Experten-Modus [953](#), [955](#), [957](#)
 Port-Verwaltung, Experten-Modus [952](#)
 Power Management, Experten-Modus [960](#)
 Quality of Service, Experten-Modus [950](#)
 System, Experten-Modus [928](#), [934](#), [938](#), [939](#),
 [942](#), [943](#), [944](#), [944](#), [946](#)
 Telefonparameter-Bereitstellung, Experten-
 Modus [957](#)
 Wiedergabegerät, Experten-Modus [957](#)
 Grundeinstellungen, Experten-Modus [918](#), [1174](#)
 Gruppen [370](#)
 Gruppen-/Sammelanschluss, Experten-Modus [1086](#)
 Gruppen-Teilnehmer, Experten-Modus [1089](#)
 Gruppen, Experten-Modus [1145](#)
 Gruppenruf [372](#)
 Anrufschutz für Gruppenmitglied [373](#)
 Rufart [375](#)
 SIP-Telefone [376](#)
 Sprachbox [374](#)

H

H.323-Stack-Trace [742](#)
 H.323-Stack-Trace, Experten-Modus [896](#)
 Halten [340](#)

Handlungsanweisung [29](#)
 Hardwaretausch [179](#)
 Hauptnetzanbieter [427](#)
 Herunterfahren von OpenScope Business X [715](#)
 Hinweise zur gleichzeitigen Nutzung von myAgent und UC Suite Clients [495](#)
 Host-Name, Experten-Modus [990](#), [1003](#)
 HotDesking [542](#)
 Hotline [453](#)
 HW-Module, Experten-Modus [1129](#)

I

ICMP (Internet Control Message Protocol) [722](#)
 IKE-SA [571](#)
 Image-Datei [709](#)
 Installation [91](#), [111](#), [129](#)
 Instant Message [265](#)
 Instant Messaging [317](#), [484](#)
 Interne Wartemusik [701](#), [703](#)
 Internes Verzeichnis (UC Smart) [253](#)
 Internes Verzeichnis (UC Suite) [293](#)
 Internet-Modem [195](#)
 Internet-Router [194](#)
 Internet-Telefonie [197](#)
 Internet-Telefonie Service Provider, Experten-Modus [1027](#)
 Internet-Telefonie-Service-Provider (ITSP) [106](#), [122](#), [197](#), [199](#)
 Internet-Zugang [192](#)
 Konfiguration [193](#)
 über externen Internet-Router [194](#)
 über externes Internet-Modem [195](#)
 Inventory OpenScope Business S [718](#)
 Inventory OpenScope Business X [717](#)
 Inventory-Management [716](#)
 IP Clients, Experten-Modus [1050](#), [1079](#)
 IP-Adressen [717](#)
 IP-Adressen-Pools, Experten-Modus [1000](#)
 IP-Adressen-Schema [95](#), [115](#)
 IP-Client (siehe IP-Teilnehmer) [216](#)
 IP-Diagnose
 Mainboard, Experten-Modus [917](#), [917](#), [918](#)
 IP-Diagnose, Experten-Modus [917](#)
 IP-Gateway-Adresse, Experten-Modus [881](#)
 IP-Mobility [542](#)
 IP-Teilnehmer [216](#)
 IPSec-Tunnel [570](#)
 ISDN Teilnehmer, Experten-Modus [1054](#)
 ISDN-Amtsleitung
 Gezielte Belegung [428](#)
 ISDN-Karte [221](#)
 ISDN-Modem [221](#)
 ISDN-Parameter, Experten-Modus [1114](#)
 ISDN-Teilnehmer [221](#)
 ISDN-Telefon [221](#)
 ITSP (Internet-Telefonie-Service-Provider) [197](#)

ITSP-Status [717](#)

J

Java [681](#)
 Java Runtime Environment (JRE) [92](#), [112](#)
 Journal
 Aufbewahrungsdauer [303](#)
 Journal (UC Smart) [260](#)
 Journal (UC Suite) [303](#)

K

Kabelanschluss [192](#)
 kanonisches Rufnummernformat [261](#)
 Kapazitäten [832](#)
 Keypad-Wahl [328](#)
 Knoten, Experten-Modus [1039](#)
 Kommende Rufe
 Rufweiterschaltungen, Experten-Modus [1098](#)
 Kommende Rufe, Experten-Modus [1085](#)
 Konferenz [262](#), [306](#), [313](#), [313](#)
 AdHoc- [310](#)
 Applikationsgesteuert [306](#)
 Arten von Konferenzen [306](#)
 Aufzeichnung [306](#)
 Authentifizierung [306](#)
 automatische Einladung per E-Mail [306](#)
 automatische Einladung per Outlook-Termin [306](#)
 Einwahlnummer [306](#)
 geplante [311](#)
 Konferenzleiter [306](#)
 Konferenzteilnehmer [306](#)
 Konferenzton [306](#)
 Mobility-Entry-Teilnehmer [306](#), [310](#), [311](#), [314](#)
 offene [314](#)
 Telefongesteuert [306](#)
 Verlängerung [306](#)
 Virtueller Konferenzraum [306](#)
 Konferenz (UC Suite) [306](#)
 Konferenz-Management [262](#), [307](#)
 Konferenz, telefongesteuert [262](#)
 Konferenzschaltung [313](#)
 Konferenzschaltung, Experten-Modus [1162](#)
 Konfiguration
 Ansagen, Experten-Modus [876](#)
 Branding, Experten-Modus [881](#)
 IP-Gateway-Adresse, Experten-Modus [881](#)
 Port-Konfiguration, Experten-Modus [877](#)
 SmartVM, Experten-Modus [877](#), [878](#), [878](#)
 Wartemusik (MoH), Experten-Modus [875](#)
 Konfiguration externe Anbieter, Experten-Modus [1148](#)
 Konfiguration, Experten-Modus [875](#), [911](#)
 Konfigurationsdaten [705](#)
 Konfigurationsdaten für die Diagnose [749](#)
 Konfigurierte Dienste, Experten-Modus [974](#)

Konfigurierte Regeln, Experten-Modus [984](#)
 Konfigurierte Tunnel, Experten-Modus [978](#)
 Konfigurierte Zertifikate, Experten-Modus [972](#)
 Konformität
 internationale Normen [47](#)
 US- und kanadische Normen [46](#)
 Kontakt [302](#)
 Konzept [29](#)
 Kunden-Trace-Protokoll [741](#)
 Kunden-Trace-Protokoll, Experten-Modus [893](#)
 Kurzwahl individuell (KWI) [332](#)
 Kurzwahl zentral (KWZ) [331](#)
 Kurzwahlziele, Experten-Modus [944](#), [1174](#)

L

Laden zum Gateway, Experten-Modus [875](#), [876](#)
 LAN 1 (WAN), Experten-Modus [990](#)
 LAN 1, Experten-Modus [1004](#)
 LAN 2, Experten-Modus [995](#), [1005](#)
 LAN 3 (Admin), Experten-Modus [996](#)
 LAN-Anforderungen [591](#)
 Lautsprecher [222](#)
 LCR
 Berechtigungen, Experten-Modus [1015](#)
 LCR-Flags, Experten-Modus [1014](#)
 Mehrere Standorte, Experten-Modus [1020](#)
 Plan, Experten-Modus [1015](#)
 Wahlregel, Experten-Modus [1018](#)
 Wegetabelle, Experten-Modus [1016](#)
 LCR (Least Cost Routing) [420](#)
 Berechtigung [425](#)
 Wahlplan [423](#)
 Wahlregeln [425](#)
 Wegetabelle [424](#)
 LCR Least Cost Routing
 Funktionalität [420](#), [420](#)
 LCR-Flags, Experten-Modus [1014](#)
 LDAP-Verbindung [681](#)
 LDAP, Experten-Modus [942](#)
 Leistungsmerkmale
 Voice, netzweit [590](#)
 Leitungen [202](#)
 Belegungsart [204](#)
 Leitungen, Experten-Modus [1100](#)
 Leitungen/Vernetzung
 ISDN-Parameter, Experten-Modus [1114](#)
 Leitungen, Experten-Modus [1100](#)
 MSN zuweisen, Experten-Modus [1114](#)
 QSIG-Leistungsmerkmale, Experten-Modus [1112](#)
 Richtung, Experten-Modus [1104](#)
 Leitungen/Vernetzung, Experten-Modus [1100](#)
 Leitungstrennung für einen Notruf [454](#)
 Leitungsvormerkmale [335](#)
 Lesende Communities, Experten-Modus [909](#)
 Lightweight CA [573](#)

Lightweight CA, Experten-Modus [969](#)
 Live Call Recording (Voice Recording; Sprachaufzeichnung) [346](#)
 Lizenz [154](#)
 über Lizenz-Autorisierungscode aktivieren [805](#)
 Lizenz-Autorisierungscode (LAC) [167](#), [174](#)
 Lizenz-Komponenten-Trace [743](#)
 Lizenz-Komponenten-Trace, Experten-Modus [899](#)
 Lizenzaktivierung [167](#), [174](#)
 Lizenzaktualisierung [179](#)
 Lizenzdatei [167](#), [174](#)
 Lizenzserver (CLS) [179](#)
 Log-Datei [747](#)
 Log-Einträge [747](#)
 LXV3, Experten-Modus [1175](#)

M

M5T-Trace-Komponente [741](#)
 M5T-Trace-Komponenten, Experten-Modus [893](#)
 Mail Exchanger [196](#), [197](#)
 Mail-Exchange-Eintrag [196](#)
 Mainboard, Experten-Modus [916](#)
 Makeln [342](#)
 Manager E [89](#)
 Manuelle Aktion [736](#)
 Mapping (Anwesenheitsstatus UC Suite) [284](#)
 Maximalwerte
 Leistungsmerkmale [842](#)
 MCL Single Stage [427](#)
 MCL Two Stage [428](#)
 MEB (Media Extension Bridge) [1178](#)
 Media Extension Bridge (MEB) [1178](#)
 Media Stream Control (MSC), Experten-Modus [1128](#)
 Mediatrix 4102S [69](#)
 Medienserver-Traces, Experten-Modus [903](#)
 Mehrsprachige Textausgabe [701](#)
 Mitteilungstexte [359](#)
 Mobile Pin [361](#)
 Mobile User Logon [542](#)
 Mobiles Logon [542](#)
 Mobility Entry [535](#)
 Leistungsmerkmal-Codes [536](#)
 Mobility Entry, Experten-Modus [1075](#)
 Mobility-Entry-Teilnehmer [313](#), [313](#)
 Konferenz [306](#), [310](#), [311](#), [314](#)
 Konferenzschaltung [262](#)
 Modem [222](#)
 MoH [701](#), [703](#)
 MSC-Statistiken, Experten-Modus [1133](#)
 MSN zuweisen, Experten-Modus [1114](#)
 Multi Location [585](#)
 Multi-SLC, Experten-Modus [1084](#)
 MX-Record [196](#)
 myAgent
 Voraussetzungen [489](#)

myPortal
 Funktionen [271](#)
 Präsenz-Status [271](#)
 myPortal for Outlook
 Funktionen [272](#)
 myPortal Smart
 Funktionen [234](#)
 myPortal to go
 Voraussetzungen [533](#)
 myReports
 Benutzerrollen [492](#)

N

Nachrichten verwalten [483](#)
 Nachrichtenübersicht [484](#)
 Nacht
 Berechtigungsgruppen, Experten-Modus [1116](#)
 Nachtschaltung, Experten-Modus [1119](#)
 Nachwahl [331](#)
 NAT (Network Address Translation) [562](#)
 NAT-Regeln [562](#)
 NAT, Experten-Modus [1008](#)
 Native SIP Server-Trunk, Experten-Modus [1041](#)
 Netzanbieter [427](#)
 Netzwerk
 Lizenz [590](#)
 Netzwerkparameter (LAN, WAN) [591](#)
 Netzwerkschnittstellen
 Application Board, Experten-Modus [1003](#), [1004](#),
[1005](#)
 Mainboard, Experten-Modus [990](#), [990](#), [995](#),
[996](#), [997](#), [998](#), [998](#), [1000](#), [1001](#), [1002](#), [1003](#)
 Netzwerkschnittstellen, Experten-Modus [990](#)
 Netzwerkverbindung prüfen [722](#)
 Neustart von OpenScape Business [714](#)
 Notrufdienst E911 [454](#)
 Notrufe
 Voraussetzungen [452](#)
 Nummerierung
 offene [593](#)
 verdeckt, geschlossen [593](#)

O

Offene Konferenz [314](#)
 Öffentliche Rufnummern im Netz [594](#)
 Online-Benutzer [760](#), [918](#)
 Online-Benutzer, Experten-Modus [918](#)
 Open Directory Service [681](#)
 Open Directory Service [675](#)
 Datenquellen, Experten Modus [1174](#), [1174](#),
[1175](#)
 Grundeinstellungen, Experten-Modus [1174](#)
 Wartung, Experten-Modus [1175](#)
 Open Directory Service, Experten-Modus [1174](#),
[1175](#), [1176](#)
 OpenScape Business Assistant [74](#), [76](#)

OpenScape Business X3R
 Schutzerdung [800](#), [801](#), [803](#)
 OpenScape Business X5R
 Schutzerdung [800](#), [801](#), [803](#)
 OpenScape Office, Experten-Modus [1174](#)
 OpenScape Personal Edition [69](#)
 OpenStage [69](#)
 OpenStage Attendant [477](#)
 OpenStage Gate View [653](#)
 OptiPoint [69](#)
 Out of Service, Experten-Modus [889](#)

P

Padding [567](#)
 Parken [340](#)
 Path Replacement [594](#)
 Payload
 Devices, Experten-Modus [1128](#)
 HW-Module, Experten-Modus [1129](#)
 Media Stream Control (MSC), Experten-Modus
[1128](#)
 Payload-SA [571](#)
 Payload, Experten-Modus [1128](#)
 PC-Clients [69](#)
 PDF-Datei
 Benachrichtigung [324](#)
 Faxnachricht [322](#)
 Peer-Zertifikate, Experten-Modus [972](#)
 Permanente Konferenz [262](#), [313](#)
 PIN zur Aktivierung eines Shutdowns [715](#)
 Ping, Experten-Modus [917](#)
 Plattform-Diagnose, Experten-Modus [916](#)
 Port [681](#)
 Port-, Baugruppen-Zustand, Experten-Modus [889](#)
 Port-Konfiguration, Experten-Modus [877](#)
 Port-Verwaltung, Experten-Modus [952](#)
 Ports [560](#)
 Portverwaltung [561](#)
 Power Management, Experten-Modus [960](#)
 PPP-Protokoll, Experten-Modus [1010](#)
 Präsenz (UC Suite) [284](#), [284](#)
 Pre-shared Keys [571](#)
 Presence (UC Smart) [251](#)
 Primary Rate Interface [428](#)
 Priorisierung von Amtsleitungen [208](#)
 Priorisierungsklassen [214](#)
 Privatleitung [335](#)
 Profil für Konfigurationsdaten von Application
 Launcher [682](#)
 Profile
 Teilnehmer [228](#)
 Profile, Experten-Modus [1170](#)
 Profile/Vorlagen, Experten-Modus [1073](#)
 PSTN-Partner, Experten-Modus [1010](#)
 PSTN, Experten-Modus [1009](#)
 Public Key Infrastructure (PKI), Experten-Modus [986](#)

Q

QSIG-Leistungsmerkmale, Experten-Modus [1112](#)
 Quality of Service (QoS) [214](#)
 Quality of Service, Experten-Modus [950](#), [1015](#)

R

R-Gesprächsschutz je Amtsleitung [419](#)
 RAS-User [216](#)
 Reaktionstabelle [748](#)
 Reaktionstabelle, Experten-Modus [905](#)
 Recycling [41](#)
 Regel [289](#)
 Regel-Editor [467](#), [505](#)
 Reload der UC Booster Card [715](#)
 Reload von OpenScape Business [714](#)
 Relocate [362](#)
 Remote Services [756](#)
 Remote-Zugang [759](#)
 Restart / Reload
 Restart / Reload, Experten-Modus [907](#)
 Restart / Reload, Experten-Modus [907](#), [907](#)
 Restart von OpenScape Business [713](#)
 Richtung, Experten-Modus [1104](#)
 Richtungen [202](#), [203](#)
 Präfix ergänzen kommend [205](#)
 Röchelschaltung [453](#)
 Routing [188](#)
 IP Routing, Experten-Modus [1006](#), [1006](#), [1007](#),
 [1007](#), [1008](#)
 NAT, Experten-Modus [1008](#)
 PSTN, Experten-Modus [1009](#), [1010](#), [1010](#)
 Routing, Experten-Modus [1006](#), [1039](#)
 rpcap Dämon, Experten-Modus [902](#)
 RPCAP-Dämon [746](#)
 Rückruf [356](#)
 Journal [303](#)
 Rückruf bei Besetzt [357](#)
 Rufeinblendung/Anklopfen [357](#)
 Rufnummernformat [261](#)
 Rufnummernplan [94](#), [116](#), [209](#), [423](#)
 Rufnummerntausch [362](#)
 Rufnummernübermittlung des Angerufenen - COLP
[338](#)
 Rufnummernübermittlung des Anrufers - CLIP [336](#)
 Rufnummernumwertung in Namen [340](#)
 Rufnummernunterdrückung des Angerufenen - COLR
[338](#)
 Rufnummernunterdrückung des Anrufers - CLIR [337](#)
 Rufsignalisierungen [336](#)
 Rufweeterschaltung im Amt [352](#)
 Rufweeterschaltung im Besetztfall [348](#)
 Rufweeterschaltung nach Zeit [348](#)
 Rufweeterschaltungen, Experten-Modus [1098](#)
 Rufzuordnung [352](#)
 Rufzuschaltung [353](#)

S

Sammelanschluss [377](#)
 Rufart [379](#)
 SIP-Telefone [380](#)
 Sprachbox [378](#)
 Schnurlose Telefone [69](#)
 Schreibende Communities, Experten-Modus [910](#)
 Secure Trace [741](#)
 Secure Trace-Einstellungen, Experten-Modus [895](#)
 Secure Trace-Zertifikat, Experten-Modus [895](#)
 Secure Trace, Experten-Modus [894](#)
 Security Associations SA [570](#)
 Security Checklist [559](#)
 Sekretär-Funktion (siehe Chef/Sekretär-Konfiguration) [386](#)
 Server-Zertifikate, Experten-Modus [988](#)
 Server, Experten-Modus [1163](#)
 Servicekennzahlen, Experten-Modus [946](#), [946](#)
 Shutdown
 PIN zur Aktivierung [715](#)
 Sicherheit
 Application Firewall, Experten-Modus [962](#)
 Deployment- und Licensing-Client (DLSC),
 Experten-Modus [963](#), [964](#), [965](#)
 Signaling- und Payload Encryption, Experten-
 Modus [967](#), [968](#), [968](#)
 SQL-Sicherheit, Experten-Modus [989](#)
 SSL, Experten-Modus [986](#), [987](#), [988](#)
 VPN, Experten-Modus [969](#), [969](#), [970](#), [971](#),
 [972](#), [972](#), [974](#), [974](#), [975](#), [978](#), [983](#), [984](#), [986](#)
 Web Sicherheit, Experten-Modus [989](#)
 Sicherheit, Experten-Modus [962](#)
 Sicherheitshinweise [30](#)
 Sicherheitshinweise für Australien [34](#)
 Sicherheitshinweise für Brasilien [35](#)
 Sicherheitshinweise für Kanada [38](#)
 Sicherheitshinweise für USA. [35](#)
 Sichern [705](#)
 sofort [707](#)
 zeitgesteuert [708](#)
 Signaling- und Payload Encryption, Experten-Modus
[967](#)
 Signaling- und Payload-Encryption (SPE) [563](#)
 Single Location [585](#)
 SIP Interconnection, Experten-Modus [1040](#)
 SIP-Client [216](#)
 SIP-Parameter, Experten-Modus [1021](#)
 SIP-Telefone [69](#)
 Site Of Operations, Experten-Modus [1137](#)
 Skin-Einstellungen, Experten-Modus [1172](#)
 SLC, Experten-Modus [1083](#)
 SmartVM, Experten-Modus [877](#), [878](#), [878](#), [1124](#)
 SMS
 Benachrichtigung [324](#)
 SMS-Benachrichtigung [325](#)
 SMS-Template [325](#)

SNMP

- Communities, Experten-Modus [909](#), [909](#), [910](#), [910](#)
- Traps, Experten-Modus [910](#)
- SNMP (Simple Network Management Protocol) [722](#)
 - Communities [723](#)
 - Management-Informationsdatenbank MIB [723](#)
 - Traps [724](#)
- SNMP Statistik, Experten-Modus [1134](#)
- SNMP, Experten-Modus [909](#)
- Sofortnachricht [265](#), [265](#), [265](#), [316](#), [316](#), [317](#)
- Sofortnachrichten [484](#)
- Software-Aktivierung [708](#)
- Software-Aktualisierung [708](#)
- Software-Image
 - System Software, Experten-Modus [881](#), [882](#), [883](#)
- Software-Image, Experten-Modus [881](#), [886](#)
- Software-Übertragung [708](#)
- Software-Update (siehe Update) [708](#)
- Sondertage, Experten-Modus [1121](#)
- SPE CA Zertifikate, Experten-Modus [968](#)
- SPE Zertifikat, Experten-Modus [968](#)
- Sprachbox [318](#)
 - Gesprächsübernahme [318](#)
 - statusbezogene Ansagen [318](#)
- Sprachbox (UC Smart) [267](#)
- Sprachbox-Gruppe [398](#)
- Sprachen [70](#)
- Sprachgateway
 - Internet-Telefonie Service Provider, Experten-Modus [1027](#)
 - SIP Interconnection, Experten-Modus [1041](#)
- Sprachgateway Codec-Parameter, Experten-Modus [1024](#)
- Sprachgateway Networking, Experten-Modus [1039](#), [1039](#)
- Sprachgateway SIP Interconnection, Experten-Modus [1040](#)
- Sprachgateway SIP-Parameter, Experten-Modus [1021](#)
- Sprachgateway Ziel-Codec-Parameter, Experten-Modus [1027](#)
- Sprachgateway, Experten-Modus [1021](#)
- Sprachnachricht
 - speichern [318](#)
- Sprachnachrichten [318](#), [484](#)
- Sprachnachrichten (UC Smart) [267](#)
- SQL-Sicherheit, Experten-Modus [989](#)
- SSDP (Smart Services Delivery Platform) [756](#)
- SSL (Secure Socket Layer) [578](#)
- Standards [1179](#)
- Standort-Liste, Experten-Modus [1162](#)
- Statische IP-Adressen, Experten-Modus [1001](#)
- Statische Routen [188](#)
- Statische Routen, Experten-Modus [1006](#), [1007](#)

Statistiken

- Gateway-Statistiken, Experten-Modus [1132](#), [1133](#)
- SNMP Statistik, Experten-Modus [1134](#)
- Telefonie-Statistiken, Experten-Modus [1134](#), [1134](#), [1135](#), [1135](#), [1136](#)
- Statistiken, Experten-Modus [1132](#)
- Status des Kommunikationssystems [716](#)
- Statusbezogene Sprachbox-Ansagen [318](#)
- Störaussendung [44](#)
- STUN (Simple Traversal of UDP over NAT) [201](#)
- Survivability [641](#)
- System Flags, Experten-Modus [919](#)
- System Texte, Experten-Modus [1134](#)
- System-Client [216](#)
- System, Experten-Modus [919](#)
- Systemsprache für Sprachbox [318](#)
- Systemtelefonbuch (UC Suite) [295](#)
- Systemverbindung [681](#)
- Systemverzeichnis [253](#)
- Systemweit, Experten-Modus [1081](#)

T

- T.38-Fax [326](#)
- Tag
 - Berechtigungsgruppen, Experten-Modus [1115](#)
- Tastenkombination für Desktop-Wahl [305](#)
- Tastenprogrammierung [224](#), [224](#)
- Tastenprogrammierung, Experten-Modus [1080](#)
- TCP- Dump, Experten-Modus [901](#)
- TCP-Dump [746](#)
- Team (siehe Teamschaltung) [382](#)
- Team-Gruppe [382](#)
 - Faxbox [384](#)
 - Rufart [384](#)
 - SIP-Telefone [384](#)
- Team/Top, Experten-Modus [1091](#)
- Teamfunktion (siehe Teamschaltung) [382](#)
- Teamschaltung [382](#)
 - Faxbox [384](#)
 - Rufart [384](#)
 - SIP-Telefone [384](#)
- Teilnehmer [209](#), [1047](#)
 - analog [222](#)
 - IP [216](#)
 - ISDN [221](#)
 - Konfiguration über Wizards [226](#)
 - Teilnehmer, Experten-Modus [1060](#), [1072](#)
- Teilnehmer Übersicht, Experten-Modus [1079](#)
- Teilnehmer-Parameter, Experten-Modus [1060](#)
- Teilnehmer-Profil [228](#)
- Teilnehmer-Status [716](#)
- Teilnehmer, Experten-Modus [1047](#), [1047](#), [1115](#), [1136](#)
- Telefon abschließen [418](#)

- Telefon-Image
 - Laden, Experten-Modus [884](#)
 - Verteilen pro Endgerät, Experten-Modus [885](#)
 - Telefon-Images
 - Verteilen, Experten-Modus [884](#)
 - Telefon-Logo
 - Laden, Experten-Modus [885](#)
 - Verteilen, Experten-Modus [886](#)
 - Telefone [69](#)
 - Telefongespräche übergeben [342](#)
 - Telefongesteuerte Konferenz [308](#)
 - Telefonie, Experten-Modus [918](#)
 - Telefonparameter-Bereitstellung, Experten-Modus [957](#)
 - Teleworking [287](#), [553](#)
 - Templates, Experten-Modus [1147](#)
 - Termin [365](#)
 - Terminalserver-/Citrix-Server-Umgebungen [271](#)
 - Texts, Experten-Modus [943](#)
 - Themen, Arten [29](#)
 - TIFF-Datei
 - Benachrichtigung [324](#)
 - Faxnachricht [322](#)
 - Top-Gruppe [386](#)
 - Faxbox [389](#)
 - Rufart [389](#)
 - SIP-Telefone [389](#)
 - Trace [738](#)
 - Protokoll [740](#)
 - Trace- Protokoll, Experten-Modus [892](#)
 - Trace-Ausgabe-Interfaces, Experten-Modus [892](#)
 - Trace-Format-Konfiguration, Experten-Modus [890](#)
 - Trace-Komponente [745](#)
 - Trace-Komponenten, Experten-Modus [900](#)
 - Trace-Konsolen-Ausgabe, Experten-Modus [916](#)
 - Trace-Profil [743](#)
 - Trace-Profile, Experten-Modus [900](#)
 - Trace:Ausgabe-Interfaces [739](#)
 - Trace:Format-Konfiguration [739](#)
 - Traceroute, Experten-Modus [918](#)
 - Traces
 - Call Supervision, Experten-Modus [897](#)
 - Digitale Prüfschleife, Experten-Modus [893](#)
 - H.323-Stack-Trace, Experten-Modus [896](#)
 - Kunden-Trace-Protokoll, Experten-Modus [893](#)
 - Lizenz-Komponenten, Experten-Modus [899](#)
 - M5T-Trace-Komponenten, Experten-Modus [893](#)
 - Medienserver-Traces, Experten-Modus [903](#)
 - rpcap Dämon, Experten-Modus [902](#)
 - Secure Trace, Experten-Modus [894](#), [895](#), [895](#)
 - TCP- Dump, Experten-Modus [901](#)
 - Trace- Protokoll, Experten-Modus [892](#)
 - Trace-Ausgabe-Interfaces, Experten-Modus [892](#)
 - Trace-Format-Konfiguration, Experten-Modus [890](#)
 - Trace-Komponenten, Experten-Modus [900](#)
 - Trace-Profile, Experten-Modus [900](#)
 - Traces, Experten-Modus [890](#)
 - Trap Communities, Experten-Modus [910](#)
 - Traps, Experten-Modus [910](#)
 - Türsprechstelle, Experten-Modus [1123](#)
 - Türsprechstelle/Türöffner [648](#)
- ## U
- Übergabe an Gruppe aus Durchsage [400](#)
 - Übermittlung kundenspezifischer Rufnummerninformation [338](#)
 - Übernahme des Write Tokens, Experten-Modus [916](#)
 - Übertragung, Software (siehe Software-Übertragung) [708](#)
 - UC Applications, Experten-Modus [1072](#)
 - UC Applikation
 - Neustart [716](#), [716](#)
 - UC Booster Card
 - Neustart [715](#), [715](#)
 - UC Smart
 - Benutzerverwaltung [1140](#)
 - Grundeinstellungen [1139](#)
 - Status [1141](#)
 - UC Smart
 - Status [755](#)
 - UC Smart Client [232](#)
 - UC Smart, Experten-Modus [1139](#)
 - UC Suite
 - Abteilungen, Experten-Modus [1145](#)
 - Benachrichtigung [753](#)
 - Benutzerverzeichnis, Experten-Modus [1142](#)
 - Client Logs [751](#)
 - Contact Center, Experten-Modus [1150](#)
 - Datei-Upload, Experten-Modus [1161](#)
 - E-Mail-Benachrichtigung [752](#)
 - Externes Verzeichnis, Experten-Modus [1147](#)
 - Faxkopfzeilen, Experten-Modus [1172](#)
 - Gruppen, Experten-Modus [1145](#)
 - Konferenzschaltung, Experten-Modus [1162](#)
 - Konfiguration externe Anbieter, Experten-Modus [1148](#)
 - Profile, Experten-Modus [1170](#)
 - Server, Experten-Modus [1163](#)
 - Skin-Einstellungen, Experten-Modus [1172](#)
 - Systemprotokolle [751](#)
 - Templates, Experten-Modus [1147](#)
 - Wartung [754](#)
 - Zeitpläne, Experten-Modus [1159](#)
 - UC Suite [1141](#)
 - Überwachung [750](#)
 - Wartung [750](#)
 - UC Suite Clients [271](#)
 - UC Suite Standort-Liste, Experten-Modus [1162](#)
 - UC Suite, Experten-Modus [1141](#)
 - UCD Agenten, Experten-Modus [1134](#)
 - UCD, Experten-Modus [1095](#)
 - Umfang für Sprachbox [318](#)

Umleiten nach Zeit [351](#)
Unfall melden [40](#)
UP0 Teilnehmer, Experten-Modus [1047](#)
Update [708](#)
 benutzerdefiniert [712](#)
Update via File Upload, Experten-Modus [882](#)
Update via Internet, Experten-Modus [881](#)
Update via USB Stick, Experten-Modus [883](#)
Upgrade [708](#)
Urlaubsplan [467](#), [505](#)

V

VBZ Gruppenzuordnung, Experten-Modus [1119](#)
VBZ Matrix, Experten-Modus [1120](#)
VBZ-Gruppen [416](#), [417](#)
 Zuordnung der KWZ-Nummern [418](#)
Verbindungsaufbau-Status [717](#)
Verbotslisten, Experten-Modus [1117](#), [1118](#)
Verhalten im Notfall [39](#), [39](#)
Verkabelung für LAN- und WAN-Anschlüsse [42](#)
Vernetzung
 homogen, nativ [584](#)
 inhomogen, hybrid [584](#)
 Knoten aus Netzwerk entfernen [643](#)
Vernetzungsplan [584](#)
Versorgungsstromkreis und Anschluss
 OpenScape Business S [42](#)
 OpenScape Business UC Booster Server [42](#)
Verzeichnis
 Sofortnachricht [265](#)
Verzeichnisse (UC Smart) [252](#)
Verzeichnisse (UC Suite) [290](#)
Virtuelle Teilnehmer, Experten-Modus [1059](#)
Virtueller Konferenzraum [262](#)
Voice-Mailbox, siehe Sprachbox [318](#)
Voicemail [318](#)
Voraussetzungen für Application Launcher [681](#)
Voraussetzungen für myAgent [489](#)
Voraussetzungen für myPortal to go [533](#)
Voraussetzungen für myReports [493](#)
VPN
 Authentifizierung [571](#)
 Bandbreiten [566](#)
 Clients [574](#)
 Sicherheitsmechanismen [570](#)
 Zertifikate [572](#)
VPN (Virtual Private Network) [565](#)
 End-to-Site [565](#)
 Site-to-Site [565](#)
VPN-Status [717](#)
VPN, Experten-Modus [969](#)

W

Wahlausendung [422](#)
Wählbares Rufnummernformat [261](#)

Wählpause [332](#)
Wahlplan, Experten-Modus [1015](#)
Wahlregel, Experten-Modus [1018](#)
Wahlregeln [425](#)
Wahlwiederholung [330](#)
WAN [196](#)
Warnhinweise [30](#)
 Gefahr [31](#)
 Hinweis [33](#)
 Vorsicht [32](#)
 Warnung [31](#)
Wartemusik [701](#), [703](#)
Wartemusik (Music On Hold MOH) bei
Anrufverteilung [408](#)
Wartung, Experten-Modus [875](#), [1175](#)
WAV-Datei
 Benachrichtigung [269](#), [324](#)
Wave-Datei [701](#), [703](#)
WBM [74](#)
 Startseite [74](#)
Web Collaboration [264](#), [315](#), [315](#), [315](#)
Web Collaboration, Experten-Modus [1173](#)
Web Services [681](#)
 Web Collaboration, Experten-Modus [1173](#)
Web Services Interface [674](#)
Web Services, Experten-Modus [1173](#)
Web Sicherheit, Experten-Modus [989](#)
Web-based Management [74](#)
Weckeinrichtung [365](#)
Wegeoptimierung [595](#)
Wegetabelle [424](#)
Wegetabelle, Experten-Modus [1016](#)
Weiterleitung, Experten-Modus [1135](#)
Wiederanruf [343](#)
Wiedergabegerät für Ansagen [1176](#)
Wiederherstellen [705](#), [708](#)
Wizards [81](#)
WLAN-Telefone [69](#)

Z

Zeitparameter, Experten-Modus [928](#)
Zeitplan [467](#), [504](#)
Zeitpläne, Experten-Modus [1159](#)
Zeitzone-Einstellungen, Experten-Modus [951](#), [952](#)
Zertifikatsgenerierung, Experten-Modus [986](#)
Zertifikatsverwaltung, Experten-Modus [970](#), [987](#)
Ziel-Codec-Parameter, Experten-Modus [1027](#)
Zifferwahl [328](#)
Zuletzt aktive Leases, Experten-Modus [1002](#)
Zurückstellen eines Rufes [354](#)
Zustand Leitung, Experten-Modus [1135](#)