



A MITEL
PRODUCT
GUIDE

Unify OpenScape Business

OpenScape Business X3/X5/X8

OpenScape Business V3

Installationsanleitung

06/2024

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Europe Limited. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos, and graphics (collectively “Trademarks”) appearing on Mitel’s Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively “Mitel), Unify Software and Solutions GmbH & Co. KG or its affiliates (collectively “Unify”) or others. Use of the Trademarks is prohibited without the express consent from Mitel and/or Unify. Please contact our legal department at iplegal@mitel.com for additional information. For a list of the worldwide Mitel and Unify registered trademarks, please refer to the website: <http://www.mitel.com/trademarks>.

© Copyright 2024, Mitel Networks Corporation

All rights reserved

Inhalt

1 Änderungsverzeichnis.....	9
1.1 Versionsgeschichte von Verbesserungen/Fixes.....	9
2 Einführung und wichtige Hinweise.....	10
2.1 Über diese Dokumentation.....	10
2.1.1 Dokumentationen und Zielgruppen.....	10
2.1.2 Arten von Themen.....	12
2.1.3 Darstellungskonventionen.....	12
2.2 Sicherheits- und Warnhinweise.....	13
2.2.1 Warnhinweise: Gefahr.....	14
2.2.2 Warnhinweise: Warnung.....	14
2.2.3 Warnungen: Vorsicht.....	15
2.2.4 Warnhinweise: Hinweis.....	16
2.2.5 Länderspezifische Sicherheitshinweise.....	17
2.2.5.1 Sicherheitshinweise für Australien.....	17
2.2.5.2 Sicherheitshinweise für Brasilien.....	18
2.2.5.3 Sicherheitshinweise für USA.....	18
2.2.5.4 Sicherheitshinweise für Kanada.....	20
2.3 Wichtige Hinweise.....	21
2.3.1 Verhalten in Notfällen.....	22
2.3.2 Bestimmungsgemäßer Gebrauch.....	22
2.3.3 Sachgemäße Entsorgung und Recycling.....	23
2.3.4 Normen und Richtlinien bezüglich der Installation.....	24
2.3.4.1 Anschluss von OpenScape Office X an den Versorgungsstromkreis.....	24
2.3.4.2 Anschluss von OpenScape Business S und OpenScape Business UC Booster Server an den Versorgungsstromkreis.....	24
2.3.4.3 Geschirmte Verkabelung für LAN- und WAN-Anschlüsse von OpenScape Business X.....	24
2.3.4.4 Brandschutzanforderungen.....	25
2.3.4.5 Blitzschutzanforderungen.....	26
2.3.4.6 Kennzeichnungen für OpenScape Business X.....	26
2.3.5 Hinweise zu Störaussendung und Funkstörung von OpenScape Business X.....	26
2.3.6 Datenschutz und Datensicherheit.....	27
2.3.7 Technische Vorschriften und Konformität von OpenScape Business X.....	28
2.3.7.1 CE-Konformität.....	28
2.3.7.2 Konformität mit US- und kanadischen Normen.....	28
2.3.7.3 Konformität mit internationalen Normen.....	29
2.3.8 Betriebsbedingungen.....	29
2.3.8.1 Betriebsbedingungen OpenScape Business X.....	29
2.3.8.2 Betriebsbedingungen OpenScape Business S und OpenScape Business UC Booster Server.....	30
3 Vorbereitungen für die Installation von OpenScape Business X3/X5/X8.....	31
3.1 Voraussetzungen für die Installation.....	31
3.2 Vorbereitende Tätigkeiten.....	36
3.2.1 Wie Sie Komponenten auspacken.....	36
3.2.2 Wie Sie die Gehäusekappe bei X3W/X5W abnehmen.....	37
4 Vorbereitungen für die Installation von OpenScape Business UC Booster Server.....	39
5 Hardwareinstallation von OpenScape Business X3W/X5W.....	40
5.1 Montageart.....	40
5.1.1 Wie Sie das Kommunikationssystem an einer Wand befestigen.....	40
5.2 Schutzerdung.....	41

5.2.1 So nehmen Sie für Schutzerdung des Hauptverteilers MDFU vor..... 42

5.2.2 Wie Sie die Schutzerdung prüfen..... 48

5.3 Anschlusskabel für den direkten Anschluss von Telefonen, Amtsleitungen usw..... 48

5.4 Konfigurationshinweise..... 49

5.4.1 Baugruppen-Steckplätze in OpenScape Business X3W..... 49

5.4.2 Steckplätze in OpenScape Business X5W..... 50

5.4.3 Baugruppeninstallation..... 52

5.4.3.1 Wie Sie eine Baugruppe stecken..... 52

5.4.3.2 Wie Sie eine Baugruppe ziehen..... 52

5.5 LAN- und WAN-Port..... 52

5.5.1 LAN- oder WAN-Anschluss durchführen..... 53

5.6 Amtsanschluss..... 54

5.6.1 Nicht für USA, Kanada: Wie Sie einen ISDN-Anlagen- oder ISDN-Mehrgeräteanschluss über eine S₀-Schnittstelle durchführen..... 54

5.6.2 Nicht für USA, Kanada: Wie Sie einen ISDN-Primärmultiplexanschluss über eine S_{2M}-Schnittstelle durchführen (nur für OpenScape Business X5W)..... 55

5.6.3 Nur für USA, Kanada: Wie Sie einen ISDN-Primärmultiplexanschluss über eine T1-Schnittstelle durchführen (nur für OpenScape Business X5W)..... 56

5.6.4 Nur für ausgewählte Länder: Wie Sie einen Amtsanschluss über eine E1-CAS-Schnittstelle durchführen (nur für OpenScape Business X5W)..... 57

5.6.5 Wie Sie einen analogen Amtsanschluss durchführen..... 57

5.7 Anschluss von Telefonen und Geräten..... 58

5.7.1 Nicht für USA, Kanada: Wie Sie ISDN-Telefone direkt anschließen..... 59

5.7.2 Nicht für USA, Kanada: Wie Sie ISDN-Telefone über den S₀-Bus anschließen..... 60

5.7.3 Wie Sie U_{P0/E}-Telefone anschließen..... 63

5.7.4 Wie Sie analoge Telefone und Geräte anschließen..... 64

5.8 Störaussendungen..... 65

5.8.1 Wie Sie einen Ferrit an der Netzanschlussleitung anbringen..... 66

5.8.2 Wie Sie Ferrite an den Peripherie-Anschlussleitungen anbringen..... 67

5.9 Abschließende Tätigkeiten..... 69

5.9.1 So setzen Sie die M.2 SSD oder die SDHC-Karte ein (System mit OCCM)..... 69

5.9.2 Wie Sie eine Sichtkontrolle durchführen..... 70

5.9.3 Wie Sie die Gehäusekappe aufsetzen..... 71

5.9.4 Wie Sie das System ans Stromnetz anschließen..... 72

6 Hardwareinstallation von OpenScape Business X3R/X5R..... 73

6.1 Montagearten..... 73

6.1.1 Wie Sie OpenScape Business X3R in einen 19"-Schrank montieren..... 73

6.1.2 Wie Sie OpenScape Business X5R in einen 19"-Schrank montieren..... 74

6.1.3 Wie Sie das Kommunikationssystem an einer Wand befestigen..... 76

6.2 Schutzerdung..... 77

6.2.1 Schutzerdung bei 19"-Schrankmontage..... 77

6.2.1.1 So stellen Sie eine Schutzerdung für das Kommunikationssystem her..... 77

6.2.1.2 Wie Sie die Schutzerdung prüfen..... 79

6.2.2 Schutzerdung bei Wandmontage und bei freier Aufstellung..... 80

6.2.2.1 So stellen Sie eine Schutzerdung für das Kommunikationssystem her..... 80

6.2.2.2 Wie Sie die Schutzerdung prüfen..... 86

6.3 Konfigurationshinweise..... 86

6.3.1 Baugruppen-Steckplätze in OpenScape Business X3R..... 86

6.3.2 Baugruppen-Steckplätze in OpenScape Business X5R..... 87

6.3.3 Baugruppeninstallation..... 87

6.3.3.1 Wie Sie eine Baugruppe stecken..... 87

6.3.3.2 Wie Sie eine Baugruppe ziehen..... 88

6.3.3.3 Wie Sie eine Abschirmblende montieren..... 88

6.4 Amtsanschluss..... 88

6.4.1 Nicht für USA, Kanada: Wie Sie einen ISDN-Anlagen- oder ISDN-Mehrgeräteanschluss über die S ₀ -Schnittstelle durchführen.....	89
6.4.2 Nicht für USA, Kanada: Wie Sie einen ISDN-Primärmultiplexanschluss über die S _{2M} -Schnittstelle durchführen (nur für OpenScape Business X5R).....	89
6.4.3 Nur für USA, Kanada: Wie Sie einen ISDN-Primärmultiplexanschluss über die T1-Schnittstelle durchführen (nur für OpenScape Business X5R).....	90
6.4.4 Nur für ausgewählte Länder: Wie Sie einen Amtsanschluss über die E1-CAS-Schnittstelle durchführen (nur für OpenScape Business X5R).....	91
6.4.5 Wie Sie einen analogen Amtsanschluss durchführen.....	91
6.5 Anschluss von Telefonen und Geräten.....	92
6.5.1 Nicht für USA, Kanada: Wie Sie ISDN-Telefone direkt anschließen.....	93
6.5.2 Nicht für USA, Kanada: Wie Sie ISDN-Telefone über den S ₀ -Bus anschließen.....	94
6.5.3 Wie Sie U _{P0/E} -Telefone anschließen.....	97
6.5.4 Wie Sie analoge Telefone und Geräte anschließen.....	98
6.6 Abschließende Tätigkeiten.....	99
6.6.1 So setzen Sie die M.2 SSD oder die SDHC-Karte ein (System mit OCCM).....	99
6.6.2 Wie Sie eine Sichtkontrolle durchführen.....	99
6.6.3 Wie Sie das System ans Stromnetz anschließen.....	100
7 Hardwareinstallation von OpenScape Business X8.....	102
7.1 Montagearten.....	102
7.1.1 Freistehende Montage.....	102
7.1.1.1 Wie Sie ein Einboxsystem aufstellen.....	102
7.1.1.2 Zweiboxsystem: Wie Sie die Systemboxen aufeinander aufstellen.....	103
7.1.1.3 Zweiboxsystem: Wie Sie die Systemboxen nebeneinander aufstellen.....	105
7.1.2 19"-Schrankmontage.....	107
7.1.2.1 So montieren Sie eine Systembox in einem 19-Zoll-Rack.....	107
7.2 Patch-Panel (optional).....	109
7.2.1 Wie Sie ein Patch-Panel in einen 19"-Schrank montieren.....	113
7.3 Schutzerdung.....	113
7.3.1 Schutzerdung bei freistehender Montage.....	114
7.3.1.1 So nehmen Sie für Schutzerdung des Hauptverteilers MDFU vor.....	114
7.3.1.2 Wie Sie die Schutzerdung prüfen.....	118
7.3.2 Schutzerdung bei 19"-Schrankmontage.....	118
7.3.2.1 So stellen Sie eine Schutzerdung für das Kommunikationssystem und das Patch-Panel her.....	118
7.3.2.2 Wie Sie die Schutzerdung prüfen.....	121
7.4 Konfigurationshinweise.....	122
7.4.1 Baugruppensteckplätze in der Basisbox.....	122
7.4.2 Baugruppen-Steckplätze in der Erweiterungsbox.....	123
7.4.3 Spezielle Baugruppensteckplätze.....	124
7.4.4 Initialisierung der Baugruppen.....	125
7.4.5 Verteilung der PCM-Highways in der Basisbox.....	125
7.4.6 Verteilung der PCM-Highways in der Erweiterungsbox.....	127
7.4.7 Zeitmultiplexkanäle der Peripheriebaugruppen.....	127
7.4.8 Baugruppeninstallation.....	129
7.4.8.1 So setzen Sie eine Baugruppe ein.....	129
7.4.8.2 So entfernen Sie eine Baugruppe.....	130
7.4.8.3 So installieren Sie Abschirmkappen.....	131
7.5 Backplanes der Systemboxen.....	132
7.5.1 Backplane der Basisbox.....	132
7.5.2 Backplane Erweiterungsbox.....	134
7.5.3 Anschluss- und Abschirm-Panels für Backplanes.....	135
7.5.3.1 Wie Sie Anschluss- oder Abschirm-Panels montieren.....	137
7.5.4 Anschluss an Backplanes.....	137
7.5.4.1 So schließen Sie das Verbindungskabel zwischen Basis- und Erweiterungsbox an (optional).....	137
7.5.4.2 So schließen Sie ein Verbindungskabel am externen Hauptverteiler an (optional).....	138

- 7.5.4.3 Wie Sie die Verbindungskabel zum Patch-Panel anschließen (optional)..... 139
- 7.5.4.4 Wie Sie die Verbindungskabel zum S₀-Patch-Panel anschließen (optional)..... 139
- 7.6 Amtsanschluss..... 142
 - 7.6.1 So richten Sie einen ISDN-Anlagenanschluss oder ISDN-Mehrgeräteanschluss über einen S₀-Port ein (nicht für USA und Kanada)..... 142
 - 7.6.2 So richten Sie einen ISDN-Primärmultiplexanschluss über einen S_{2M}-Port ein (nicht für USA und Kanada)..... 143
 - 7.6.3 So richten Sie einen ISDN-Primärmultiplexanschluss über eine T1-Schnittstelle ein (nur für USA und Kanada)..... 144
 - 7.6.4 Nur für ausgewählte Länder: Wie Sie einen Amtsanschluss über eine E1-CAS-Schnittstelle durchführen..... 145
 - 7.6.5 So richten Sie eine analoge Amtsleitung ein..... 145
- 7.7 Anschluss von Telefonen und Geräten..... 146
 - 7.7.1 So schließen Sie ISDN-Telefone direkt an (nicht für USA und Kanada)..... 147
 - 7.7.2 So schließen Sie ISDN-Telefone über den S₀-Bus an (nicht für USA und Kanada)..... 148
 - 7.7.3 So schließen Sie U_{P0/E}-Telefone an..... 151
 - 7.7.4 So schließen Sie analoge Telefone und Geräte an..... 152
- 7.8 Abschließende Tätigkeiten..... 153
 - 7.8.1 So setzen Sie die M.2 SSD oder die SDHC-Karte ein (System mit OCCM)..... 154
 - 7.8.2 So nehmen Sie eine Sichtprüfung vor..... 154
 - 7.8.3 Nur bei freistehender Montage: Wie Sie die Kunststoffabdeckungen einer Systembox montieren..... 156
 - 7.8.4 Wie Sie das System ans Stromnetz anschließen..... 156
- 8 Installation des Linux-Servers..... 157**
 - 8.1 Voraussetzungen..... 157
 - 8.2 Installation in einer virtuellen Umgebung..... 160
 - 8.2.1 VM Co-Residency und QoS-Richtlinie..... 162
 - 8.2.2 Zeitsynchronisation des Gastbetriebssystems Linux..... 163
 - 8.2.2.1 Wie Sie die Zeitsynchronisation für das Gastbetriebssystem Linux in VMWare konfigurieren..... 163
 - 8.3 Linux-Sicherheitsaspekte und RAID-Verbund..... 164
 - 8.4 Erstinbetriebnahme ohne Software-RAID..... 166
 - 8.4.1 SLES 12 SP5 ohne Software-RAID installieren und konfigurieren..... 166
 - 8.4.2 Wie Sie von SLES 11 auf SLES 12 SP5 aktualisieren..... 170
 - 8.4.3 Wie Sie von SLES 12 SP3 auf SLES 12 SP5 aktualisieren..... 171
 - 8.5 Erstinbetriebnahme mit Software-RAID..... 172
 - 8.5.1 Wie Sie das BIOS RAID deaktivieren..... 173
 - 8.5.2 Wie Sie SLES 12 SP5 Software-RAID installieren und konfigurieren..... 173
 - 8.6 Konfiguration einer einheitlichen Zeitbasis..... 178
 - 8.6.1 Wie Sie einen SNTP-Server konfigurieren..... 178
 - 8.7 Updates..... 179
 - 8.7.1 Wie Sie automatische Online-Updates aktivieren..... 180
 - 8.7.2 Online-Updates manuell aktivieren..... 180
 - 8.8 Sicherung und Wiederherstellung der Serversoftware..... 181
- 9 Ersteinrichtung von OpenScope Business X..... 182**
 - 9.1 Voraussetzungen für die Erstinstallation..... 182
 - 9.2 Komponenten..... 183
 - 9.3 Rufnummernplan..... 185
 - 9.4 IP-Adressen-Schema..... 186
 - 9.5 Erstinbetriebnahme..... 187
 - 9.5.1 Wie Sie das Kommunikationssystem starten..... 188
 - 9.5.2 Wie Sie den Admin-PC mit dem Kommunikationssystem verbinden..... 188
 - 9.5.3 Wie Sie das WBM starten..... 189
 - 9.6 Integration ins Kunden-LAN..... 191
 - 9.6.1 Wie Sie den Wizard Erstinstallation starten..... 191
 - 9.6.2 Systemeinstellungen..... 192

9.6.2.1	Wie Sie das Display-Logo und die Produktbezeichnung festlegen.....	192
9.6.2.2	Wie Sie die IP-Adressen festlegen (optional).....	193
9.6.2.3	So legen Sie Richtungsnamen fest.....	194
9.6.3	DHCP-Einstellungen	194
9.6.3.1	Wie Sie den internen DHCP-Server deaktivieren.....	195
9.6.3.2	Wie Sie den internen DHCP-Server aktivieren und konfigurieren.....	196
9.6.4	Länder- und Zeiteinstellungen.....	197
9.6.4.1	Wie Sie das Länderkennzeichen und die Sprache für Event-Logs auswählen.....	198
9.6.4.2	Wie Sie die DECT-Systemkennung eingeben.....	198
9.6.4.3	Wie Sie das Datum und die Uhrzeit manuell einstellen.....	199
9.6.4.4	Wie Sie das Datum und die Uhrzeit von einem SNTP-Server beziehen.....	200
9.6.5	UC-Lösung.....	200
9.6.5.1	Wie Sie die UC-Lösung festlegen.....	201
9.6.6	Anschluss des Kommunikationssystems ans Kunden-LAN.....	202
9.6.6.1	Wie Sie das Kommunikationssystem ans Kunden-LAN anschließen.....	202
9.7	Basiskonfiguration.....	202
9.7.1	Wie Sie den Wizard Basisinstallation starten.....	203
9.7.2	Systemrufnummern und Vernetzung.....	203
9.7.2.1	Wie Sie die Systemrufnummern für einen Anlagenanschluss eingeben.....	204
9.7.2.2	Wie Sie die Systemrufnummern für einen Mehrgeräteanschluss eingeben.....	205
9.7.2.3	Wie Sie die Vernetzung aktivieren oder deaktivieren.....	206
9.7.3	Teilnehmerdaten.....	206
9.7.3.1	Wie Sie die Teilnehmerdaten anzeigen.....	208
9.7.3.2	Wie Sie alle Rufnummern löschen.....	208
9.7.3.3	Wie Sie vorkonfigurierte Rufnummern an den individuellen Rufnummernplan anpassen.....	208
9.7.3.4	Wie Sie die Teilnehmerdaten über eine XML-Datei importieren.....	209
9.7.3.5	Anzeigen von Massendaten.....	209
9.7.4	ISDN-Konfiguration	211
9.7.4.1	Wie Sie den Anschluss von ISDN-Teilnehmern konfigurieren.....	211
9.7.4.2	Wie Sie den ISDN-Anlagenanschluss konfigurieren.....	212
9.7.4.3	Wie Sie den ISDN-Mehrgeräteanschluss konfigurieren.....	212
9.7.4.4	Wie Sie die ISDN-Konfiguration deaktivieren.....	213
9.7.5	Internet-Zugang	213
9.7.5.1	Wie Sie den Internet-Zugang über einen externen Internet-Router über den LAN-Anschluss konfigurieren.....	215
9.7.5.2	Wie Sie den Internet-Zugang über einen externen Internet-Router über den WAN-Anschluss konfigurieren.....	215
9.7.5.3	Wie Sie den Internet-Zugang über einen vorkonfigurierten ISP konfigurieren.....	216
9.7.5.4	Internet-Zugang über Standard-ISP PPPoE konfigurieren.....	218
9.7.5.5	Wie Sie den Internet-Zugang über einen Standard-ISP PPTP konfigurieren.....	220
9.7.5.6	Wie Sie den Internet-Zugang deaktivieren.....	223
9.7.6	Internet-Telefonie	223
9.7.6.1	Vordefinierten ITSP konfigurieren.....	224
9.7.6.2	Wie Sie die Internet-Telefonie deaktivieren.....	229
9.7.7	Teilnehmer.....	229
9.7.7.1	ISDN-Teilnehmer konfigurieren	230
9.7.7.2	Analoge Teilnehmer konfigurieren	232
9.7.7.3	UP0-Teilnehmer konfigurieren	235
9.7.7.4	Wie Sie DECT-Teilnehmer konfigurieren.....	238
9.7.7.5	Wie Sie IP- und SIP-Teilnehmer konfigurieren.....	241
9.7.8	Konfiguration von UC Suite.....	244
9.7.8.1	Wie Sie UC Suite konfigurieren.....	244
9.7.9	Konfiguration der UC Smart Sprachboxen.....	245
9.7.9.1	Wie Sie die UC Smart Sprachboxen konfigurieren.....	245
9.7.10	Konferenz-Server-Einstellungen.....	246
9.7.10.1	Wie Sie die Konferenz-Server-Einstellungen ändern.....	246

9.7.11 E-Mail-Versand (optional).....	246
9.7.11.1 E-Mail-Versand konfigurieren.....	246
9.8 Abschließende Tätigkeiten.....	249
9.8.1 Wie Sie die Lizenzen aktivieren und zuordnen.....	250
9.8.2 Wie Sie den UC Smart Client zur Installation bereitstellen.....	253
9.8.3 Wie Sie die UC Suite Clients zur Installation bereitstellen.....	253
9.8.4 Wie Sie eine Datensicherung durchführen.....	255
9.9 Inbetriebnahme der IP-Telefone.....	255
9.9.1 Wie Sie ein IP-Telefon konfigurieren.....	257
9.9.2 Wie Sie ein SIP-Telefon konfigurieren.....	258
10 Ersteinrichtung OpenScape Business UC Booster.....	260
10.1 Voraussetzungen für die Ersteinrichtung.....	262
10.2 Sicherung der Konfigurationsdaten des Kommunikationssystems.....	265
10.2.1 Wie Sie eine Datensicherung durchführen.....	265
10.3 Inbetriebnahme UC Booster Card.....	266
10.3.1 Montage der UC Booster Card.....	266
10.3.2 Konfiguration der UC Booster Card.....	267
10.3.3 Software-Update für die UC Booster Card.....	267
10.3.3.1 Wie Sie ein Software-Update durchführen.....	267
10.4 Inbetriebnahme UC Booster Server.....	268
10.4.1 Installation der Kommunikationssoftware.....	268
10.4.1.1 Kommunikationssoftware auf einem Linux-Server oder in einer virtuellen Umgebung installieren.....	269
10.4.2 Konfiguration des UC Booster Servers.....	271
10.4.2.1 IP-Adresse des Kommunikationssystems bekannt geben.....	271
10.4.3 Software-Update für die UC Booster Card.....	273
10.5 Basiskonfiguration.....	274
10.6 Abschließende Tätigkeiten.....	274
10.7 Deinstallation der Kommunikationssoftware.....	275
10.7.1 Wie Sie die Kommunikationssoftware deinstallieren.....	275
10.8 Hochrüstung von UC Booster Card auf UC Booster Server.....	275
10.9 Verwendete Ports.....	277
11 Nicht mehr angebotene Komponenten.....	280
11.1 Hauptverteiler MDFU (optional).....	280
11.1.1 Wie Sie den Hauptverteiler MDFU an einer Wand befestigen.....	281
11.2 Verbindungskabel zum externen Hauptverteiler (optional).....	281
11.2.1 So schließen Sie ein Verbindungskabel am externen Hauptverteiler an (optional).....	283
Index.....	287

1 Änderungsverzeichnis

Die in der folgenden Liste genannten Änderungen sind kumulativ.

Änderungen in V3R2 FR1

Betroffene Kapitel	Beschreibung der Änderung
E-Mail-Versand konfigurieren auf Seite 246	Support für OAuth 2.0-Authentifizierung

1.1 Versionsgeschichte von Verbesserungen/Fixes

Die in der diesem Kapitel genannten Änderungen sind kumulativ.

Änderungen in V3R3 FR2

Servicefall-ID	Datum der Änderung	Beschreibung der Änderung	Betroffene Kapitel
PRB000076122	13 Juni 2024	Erhöhen Sie die Anzahl der Ditamap-Ausgänge auf 8	-

Änderungen in V3R1

Servicefall-ID	Datum der Änderung	Beschreibung der Änderung	Betroffene Kapitel
PRB000052823	21 April 2021	Aktualisierte Tabelle mit den Mindestanforderungen für die Installation des Kommunikationssystems in einer VM.	Installation in einer virtuellen Umgebung auf Seite 160

2 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.

2.1 Über diese Dokumentation

Diese Dokumentation informiert Sie über die Hardwareinstallation und Ersteinrichtung der Hardwaremodelle OpenScape Business X3/X5/X8.

Die Angaben in dieser Dokumentation sind ausschließlich als begleitende Informationen zu sehen und ersetzen keine Schulung.

Dieses Dokument richtet sich an Administratoren und Servicetechniker.

Informationen, die über den Inhalt dieses Dokuments hinausgehen, finden Sie in der *OpenScape Business Servicedokumentation* und der *OpenScape Business Administratordokumentation*.

2.1.1 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, 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, 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.

Einführung und wichtige Hinweise

- 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.

2.1.2 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 ...

2.1.3 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

Art der Information	Darstellung	Beispiel
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>

2.2 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.

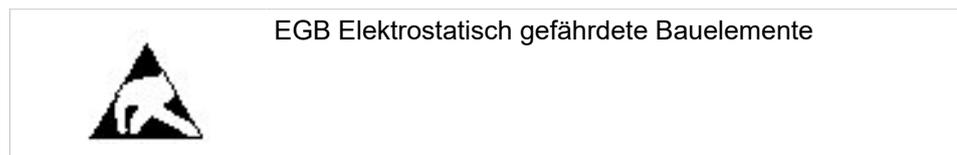


ACHTUNG: Kennzeichnet gefährliche Situation, die Verletzungen zur Folge haben kann.

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.



2.2.1 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.

2.2.2 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.
- 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.

2.2.3 Warnungen: Vorsicht

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



ACHTUNG: 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.



ACHTUNG: 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.



ACHTUNG: 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.
-

2.2.4 Warnhinweise: Hinweis

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

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

- Prüfen Sie vor der Inbetriebnahme, ob die Nennspannung der Netzspannungsversorgung mit der Nennspannung des Kommunikationssystems oder Servers übereinstimmt (Typenschild).
- Befolgen Sie folgende EGB-Maßnahmen zum Schutz der elektrostatisch gefährdeten Bauelemente:
 - Legen Sie vor allen Arbeiten an Baugruppen und Modulen das Erdungsarmband ordnungsgemäß an.
 - Legen Sie Baugruppen und Module immer auf einer geerdeten, leitfähigen Unterlage ab.
 - Transportieren und versenden Sie Komponenten des Kommunikationssystems (zum Beispiel Baugruppen) nur in geeigneten Verpackungen.
- Verwenden Sie ausschließlich Originalzubehör. Bei Nichtbeachtung können Beschädigungen am Kommunikationssystem auftreten oder Sicherheits- und EMV-Bestimmungen verletzt werden.

- Bei einer plötzlichen Temperaturänderung kann die Luftfeuchtigkeit kondensieren. Wird ein Kommunikationssystem oder Server beispielsweise aus kalter Umgebung in warme Räume gebracht, kann Feuchtigkeit kondensieren. Warten Sie, bis die Temperatur ausgeglichen ist und das Kommunikationssystem oder der Server absolut trocken ist, bevor Sie es in Betrieb nehmen.
- Schließen Sie alle Leitungen nur an den vorgegebenen Anschlusspunkten an.
- Wenn keine Notstromversorgung verfügbar ist oder bei Stromausfall nicht auf analoge Notfalltelefone umgeschaltet werden kann, lassen sich bei einem Ausfall der Stromversorgung keine 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.

2.2.5 Länderspezifische Sicherheitshinweise

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

2.2.5.1 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.

2.2.5.2 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.

2.2.5.3 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 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.

2.2.5.4 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.

2.3 Wichtige Hinweise

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

2.3.1 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 Wiederbelebensmaßnahmen 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?
- 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.

2.3.2 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.

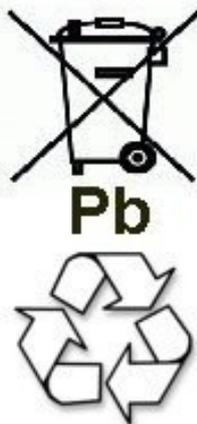
Anmerkung: Reinigen Sie das Gehäuse von Kommunikationssystem und Server nur mit einem weichen, leicht feuchten Tuch. Benutzen Sie keine scharfen Reiniger oder Scheuerschwämme.

2.3.3 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.

2.3.4 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.

2.3.4.1 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 Schutz- und Neutralleiter aufgeteilt ist. TN-S und TN-C-S gemäß Definition der Norm IEC 364-3.

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

2.3.4.2 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.

2.3.4.3 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.^{***)}

2.3.4.4 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.

<p>IEC 60332-1 Hinweis: IEC 60332-1 entspricht der Prüfmethode UL VW-1</p>	<p>EN 60332-1-1 und EN 60332-2-1</p>	<p>DIN EN 60332-1-1 (VDE 0482-332-1-1) und DIN EN 60332-2-1 (VDE 0482-332-2-1)</p>
--	--------------------------------------	--

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.

*) 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).

2.3.4.5 Blitzschutzanforderungen

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

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).

2.3.4.6 Kennzeichnungen für OpenScape Business X



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

2.3.5 Hinweise zu Störaussendung und Funkstörung von OpenScape Business X

Die Kommunikationssysteme OpenScape Business X sind Einrichtungen der Klasse B gemäß EN 55032.

2.3.6 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 der Datenschutzgrundverordnung (DSGVO) und 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 Sicherungs-CDs-/DVDs oder Protokollausdrucke. Das gilt sowohl für den Serviceeinsatz, als auch für Lagerung und Transport.

- Sorgen Sie dafür, dass nicht mehr benötigte Datenträger vollständig vernichtet werden. Vergewissern Sie sich, dass keine Papiere allgemein zugänglich zurückbleiben.
- Arbeiten Sie mit Ihren Ansprechpartnern beim Kunden zusammen: Das schafft Vertrauen und entlastet Sie selbst.

2.3.7 Technische Vorschriften und Konformität von OpenScape Business X

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

2.3.7.1 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)

2.3.7.2 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.

2.3.7.3 Konformität mit internationalen Normen

	Normenreferenz
Safety	IEC 60950-1 und IEC 62368-1
EMC Emission	CISPR 32

2.3.8 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).

2.3.8.1 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.

2.3.8.2 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.

3 Vorbereitungen für die Installation von OpenScape Business X3/X5/X8

Bevor OpenScape Business X3/X5/X8 Kommunikationssysteme eingerichtet und erstmalig in Betrieb genommen werden können, muss ein geeigneter Installationsstandort gefunden werden, der mit den Betriebsbedingungen übereinstimmt (siehe [Betriebsbedingungen OpenScape Business X](#)). Zudem sind vorbereitende Tätigkeiten auszuführen.

3.1 Voraussetzungen für die Installation

Für die Installation der Kommunikationssysteme OpenScape Business X3/X5/X8 sind verschiedene Werkzeuge und Hilfsmittel erforderlich. Bei der Auswahl des Montagestandorts sind bestimmte Anforderungen zu beachten. Für den Einsatz der Kommunikationssysteme in den USA und in Kanada gelten besondere Anforderungen für den Netzspannungsanschluss.

OpenScape Business X3W und OpenScape Business X5W können ausschließlich an einer Wand montiert werden.

OpenScape Business X3R und OpenScape Business X5R sind Kommunikationssysteme im 19"-Rackgehäuse, die in einen 19"-Schrank montiert, frei aufgestellt (Tischbetrieb) oder an einer Wand montiert werden können.

OpenScape Business X8 ist ein modulares Kommunikationssystem, das als Einboxsystem (Basisbox) oder als Zweiboxsystem (Basisbox + Erweiterungsbox) eingesetzt werden kann. OpenScape Business X8 kann frei aufgestellt oder in einen 19"-Schrank montiert werden.

Achtung: Die Installation der Kommunikationssysteme darf ausschließlich durch autorisiertes Fachpersonal durchgeführt werden.

Werkzeuge und Hilfsmittel

Folgende Werkzeuge und Hilfsmittel werden benötigt:

- Seitenschneider, Telefonzange, Abisolierzange, Flachzange
- Schlitzschraubendrehersatz
- Kreuzschraubendrehersatz Pozidriv
- TORX-Schraubendrehersatz
- Meterstab
- Ring- oder Gabelschlüssel 8 mm, Gabelschlüssel 13 mm (nur für X8)
- Baugruppenschlüssel (nur für X8)
- Bohrmaschine, Hammer, Wasserwaage (nur für die Wandmontage)
- Auflegewerkzeug für Trenn- und Rangierleisten in Hauptverteiltern
- Digital-Multimeter, um Schutzleiterverbindungen sowie Teilspannungen zu prüfen

Allgemeine Voraussetzungen für die Auswahl des Montagestandorts

Folgende Vorgaben sind bei der Auswahl des Montagestandorts unbedingt zu beachten:

- Das Kommunikationssystem (und der 19"-Schrank) darf keiner direkten Wärmeeinwirkung ausgesetzt werden (zum Beispiel durch Sonneneinstrahlung oder Heizkörper).
- Das Kommunikationssystem (und der 19"-Schrank) darf keiner übermäßigen Staubeinwirkung ausgesetzt werden.
- Chemikalische Einflüsse auf das Kommunikationssystem (und der 19"-Schrank) müssen vermieden werden.
- Während des Betriebs muss eine Kondensation von Luftfeuchtigkeit auf oder im Kommunikationssystem unter allen Umständen vermieden werden.

Das Kommunikationssystem muss absolut trocken sein, bevor es in Betrieb genommen werden darf.

- Standard-Teppichbeläge müssen vermieden werden, da diese elektrostatische Ladungen produzieren.
- Die klimatischen und mechanischen Bedingungen für den Betrieb des Kommunikationssystems müssen beachtet werden (siehe [Betriebsbedingungen OpenScape Business X](#)).
- Der Stecker des Netzanschlusskabels muss leicht zugänglich sein, damit jederzeit eine schnelle Trennung des Kommunikationssystems von der Netzspannung möglich ist.
- Für einen Hauptverteiler oder sonstige Zusatzeinrichtungen muss ausreichend Platz berücksichtigt werden.
- Nur für USA, Kanada: Der Abstand zwischen Geräten der Unify GmbH & Co. KG und anderen Elektrogeräten muss mindestens 101,6 cm (40") betragen. Laut National Electrical Code NEC ist an der Vorderseite von Elektrogeräten ein Mindestabstand von 91,4 cm (36") einzuhalten sowie ein Abstand von 101,6 cm (40") zu anderen Elektroinstallationen.

Spezielle Voraussetzungen bei bei X3R/X5R für die Auswahl des Montagestandorts

Folgende Vorgaben sind bei der Auswahl des Montagestandorts unbedingt zu beachten:

- Ein Mindestabstand von 10 cm zum Gehäuse muss freigehalten werden, um eine ausreichende Belüftung eines Kommunikationssystems zu gewährleisten.

Spezielle Voraussetzungen bei X3W/X5W für die Auswahl des Montagestandorts

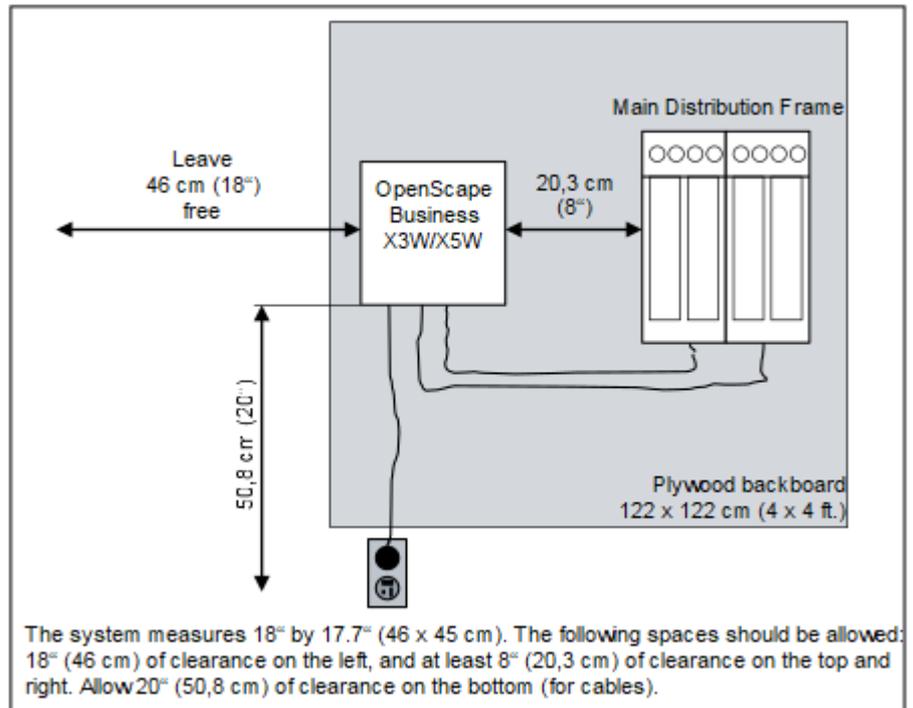
Folgende Vorgaben sind bei der Auswahl des Montagestandorts für die Wandmontage unbedingt zu beachten:

- Folgende Mindestabstände zum Gehäuse müssen freigehalten werden, um eine ausreichende Belüftung eines Kommunikationssystems zu gewährleisten:
 - Linke Seite: 30 cm (für den Baugruppensevice)
 - Rechte Seite, oben und unten: Jeweils 10 cm
- Nur für USA, Kanada: Der Raum, in dem ein Kommunikationssystem montiert wird, muss ausreichend Platz für Installations- und

Vorbereitungen für die Installation von OpenScape Business X3/X5/X8

Wartungsarbeiten bieten (zum Beispiel für das Abnehmen und Aufsetzen der Gehäusekappe). Das folgende Bild zeigt die Platzanforderungen.

Empfohlen wird die Verwendung einer Sperrholzplatte mit einer Mindeststärke von 127 mm (0,5") und den Mindestabmessungen 122 x 122 cm (4 ft. x 4 ft.).



Spezielle Voraussetzungen bei X8 für die Auswahl des Montagestandorts bei freistehender Montage

Folgende Vorgaben sind bei der Auswahl des Montagestandorts bei einer freistehenden Montage unbedingt zu beachten:

- Ein Mindestabstand von 50 mm zwischen Unterkante einer Systembox und Boden und zwischen übereinander montierten Systemboxen muss eingehalten werden, um eine ausreichende Belüftung der Systemboxen zu gewährleisten.
- Bei übereinander montierten Systemboxen muss die Basisbox immer als untere Box eingesetzt werden.
- Vor und hinter den Systemboxen muss ein Mindestabstand von jeweils 10 cm freigehalten werden, um den Baugruppenservice und die Verkabelung zu ermöglichen.

Spezielle Voraussetzungen bei X8 für die Auswahl des Montagestandorts bei 19"-Schrankmontage

Folgende Vorgaben sind bei der Auswahl des Montagestandorts bei einer 19"-Schrankmontage unbedingt zu beachten:

Vorbereitungen für die Installation von OpenScape Business X3/X5/X8

- Der oder die für den Einbau des Kommunikationssystems OpenScape Business X8 vorgesehenen 19"-Schränke müssen folgende Eigenschaften aufweisen:
 - Einbauten im 19"-Schrank müssen von vorne und von hinten zugänglich sein.
 - Der Einbau von Komponenten muss an der Vorder- und an der Rückseite des 19"-Schanks möglich sein (mindestens vier vertikale Holme).
 - Eine Schrankbreite von 70 bis 80 cm und eine Schranktiefe von mindestens 60 cm wird empfohlen. Größere Schranktiefen (80 bis 90 cm) ermöglichen eine einfachere Montage, einen komfortableren Kabelservice und den Einbau weiterer Komponenten in der Schrankrückseite.
 - Die für den Einbau der Systemboxen notwendigen Auflagewinkel müssen eine Mindesttraglast von 40 kg aufweisen. Die Auflagewinkel sind vom Lieferanten des 19"-Schanks zu beziehen.
 - Die Systemboxen sind mit den zum Lieferumfang gehörenden Haltewinkeln an den Schrankholmen zu befestigen.
- Durch die an der Oberseite der Systemboxen angebrachte graue Kunststoffblende muss eine Höheneinheit (eine Höheneinheit entspricht ca. 1,7" = 43 mm) oberhalb einer Systembox freibleiben. Die Kunststoffblende darf auf keinen Fall entfernt werden!
- Um eine ausreichende Wärmeabfuhr zu gewährleisten, darf die Basisbox nur an unterster Stelle in einem 19"-Schrank montiert werden. Bei einem 19"-Schrank mit bereits eingebauten aktiven Komponenten (wärmeabgebende Komponenten) ist der unterste Bereich für die Montage der Basisbox freizumachen. Handelt es sich um inaktive Komponenten (zum Beispiel Patch-Panels), darf die Basisbox auch darüber montiert werden.

Vorbereitungen für die Installation von OpenScape Business X3/X5/X8

- Um eine ausreichende Belüftung der Systemboxen innerhalb eines 19"-Schranks zu gewährleisten, müssen folgende Mindestabstände freigehalten werden:
 - Drei Höheneinheiten zwischen zwei übereinander montierten Systemboxen.
 - Eine Höheneinheit oberhalb einer Systembox, falls zum Beispiel ein Patch-Panel montiert wird.

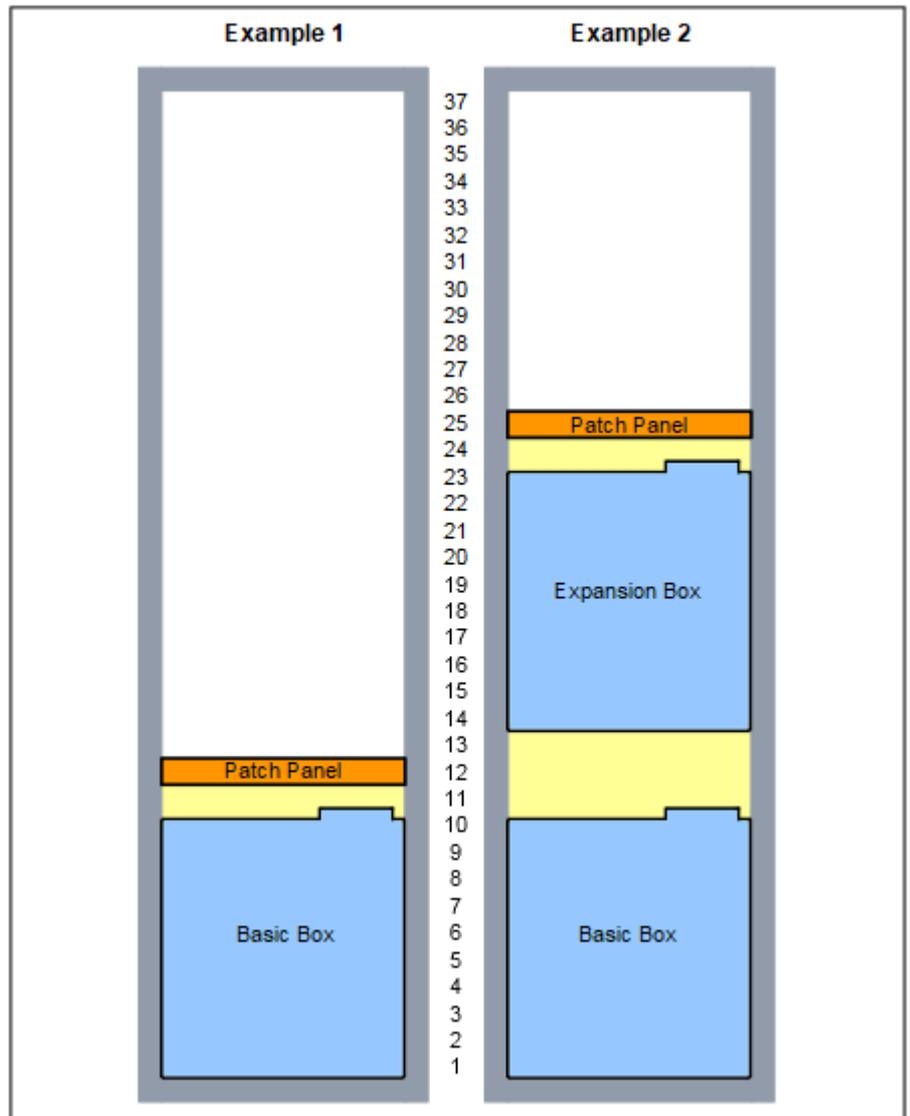


Abbildung 1: OpenScape Business X8 – Beispiele für eine 19"-Schrankschrankhöhe von 1,92 m (37 Höheneinheiten)

Nur für USA, Kanada: Voraussetzungen für den Netzspannungsanschluss

Der Netzspannungsanschluss für die Kommunikationssysteme muss folgende Anforderungen erfüllen:

Vorbereitungen für die Installation von OpenScape Business X3/X5/X8

Vorbereitende Tätigkeiten

- Elektrische Anschlusswerte:

Nennspannung	Nennspannungsbereich		Nennfrequenzbereich		Anschlussdosen-Konfigurationen
	von	bis	von	bis	
120 V AC/60 Hz	110 V AC	130 V AC	47 Hz	63 Hz	NEMA 5-15, 2polig, 3-Draht, Erde

- Nur für X8: Zwischen Steckdose und Kommunikationssystem muss ein UL-gelisteter oder CSA-zertifizierter Überspannungsschutz geschaltet werden. Pro Überspannungsschutz können maximal zwei Systemboxen angeschlossen werden.

Anmerkung: Der direkte Anschluss des Kommunikationssystems OpenScape Business X8 an eine Steckdose ist verboten!

- Nur für X3/X5: Zwischen Steckdose und Kommunikationssystem sollte ein Überspannungsschutz geschaltet werden.
- Nur für X8: Die Spannungsquelle darf nicht weiter als 2,4 m (8 ft.) vom Kommunikationssystem entfernt sein und muss eine Spannung von 120 V AC (einphasig, abgesichert) bei 50 bis 60 Hz und 20 A liefern.
- Nur für X3/X5: Die Spannungsquelle darf nicht weiter als 2 m (6 ft.) vom Kommunikationssystem entfernt sein und muss eine Spannung von 120 V AC (einphasig, abgesichert) bei 50 bis 60 Hz liefern.
- Für jedes Kommunikationssystem sollte ein eigener Stromkreis mit isoliertem Schutzleiter verwendet werden.
- Am Hauptschalter der Netzspannungsversorgung sollte ein Warnhinweis angebracht werden, um ein versehentliches Abschalten der Stromversorgung eines Kommunikationssystems zu verhindern.

3.2 Vorbereitende Tätigkeiten

Vor der eigentlichen Montage sind die gelieferten Komponenten auszupacken und zu überprüfen.

Auf dem Mainboard befindet sich ein Akku, der zur Pufferung von Datum und Uhrzeit dient. Es ist möglich, dass Mainboards älteren Stands noch mit einer Akku-Schutzfolie ausgeliefert wurden. Vor der Inbetriebnahme des Kommunikationssystems muss diese Schutzfolie entfernt werden.

Ab folgenden Ausgabezuständen wird keine Akku-Schutzfolie mehr verwendet:

- S30810-Q2959-X-6 (OCCM)
- S30810-Q2959-Z-5 (OCCMR)
- S30810-Q2962-X-7 (OCCL)

3.2.1 Wie Sie Komponenten auspacken

Packen Sie das Kommunikationssystem und die mitgelieferten Teile wie folgt aus:

Schritt für Schritt

- 1) Öffnen Sie die Verpackungen ohne den Inhalt zu beschädigen.
 - 2) Prüfen Sie die zum Lieferumfang gehörenden Komponenten anhand des Lieferscheins auf Vollständigkeit.
 - 3) Melden Sie eventuell aufgetretene Transportschäden an die auf dem Lieferschein genannte Adresse.
 - 4) Entsorgen Sie das Verpackungsmaterial entsprechend den länderspezifischen Bestimmungen.
-



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen
Benutzen Sie Kommunikationssysteme, Geräte und Betriebsmittel nur im einwandfreien Zustand. Die Inbetriebnahme von Geräten mit äußeren Beschädigungen ist verboten.

3.2.2 Wie Sie die Gehäusekappe bei X3W/X5W abnehmen

Schritt für Schritt

- 1) Lösen Sie die beiden Schraubverschlüsse der Gehäusekappe mit einem Schlitzschraubendreher.
 - 2) Ziehen Sie die Gehäusekappe ab.
-



ACHTUNG: Schnittwunden durch scharfkantiges Abschirmblech

Vorbereitungen für die Installation von OpenScape Business X3/X5/X8

Fassen Sie die Gehäusekappe nur von außen. Ansonsten können Schnittwunden durch das eventuell scharfkantige Abschirmblech an der Innenseite der Gehäusekappe hervorgerufen werden.



4 Vorbereitungen für die Installation von OpenScape Business UC Booster Server

Bevor der OpenScape UC Business Booster Server installiert und erstmalig in Betrieb genommen werden kann, sind einige vorbereitende Tätigkeiten auszuführen.

Der UC Booster Server wird nur in Verbindung mit den folgenden Mainboards unterstützt:

- OCCM
- OCCMR
- OCCL

Für das folgende System ist kein UC Booster Server erforderlich:

- OCCMA
- OCCMB
- OCCMRA
- OCCMRB
- OCCLA

Für OpenScape UC Business Booster Server wird die OpenScape Business Kommunikationssoftware auf einem Linux-Server installiert.

Die Voraussetzungen für den Linux-Server und die Installation des Linux-Betriebssystems finden Sie unter [Installation des Linux-Servers](#) auf Seite 157.

Die Voraussetzungen für den OpenScape Business UC Booster Server und die Installation der OpenScape Business Kommunikationssoftware finden Sie unter [Ersteinrichtung OpenScape Business UC Booster](#) auf Seite 260.

5 Hardwareinstallation von OpenScape Business X3W/ X5W

Beschrieben ist die vorwiegend durchgeführte Standardmontage der Kommunikationssysteme OpenScape Business X3W und OpenScape Business X5W.

OpenScape Business X3W und OpenScape Business X5W können ausschließlich an einer Wand montiert werden.



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

- Arbeiten am geöffneten Gehäuse dürfen nur im spannungsfreien Zustand durchgeführt werden.
- Prüfen Sie vor Beginn jeder Arbeit, ob alle Stromkreise spannungsfrei sind. Halten Sie es nie für selbstverständlich, dass mit Ausschalten einer Sicherung oder eines Hauptschalters alle Stromkreise auch zuverlässig unterbrochen sind.

5.1 Montageart

Die Kommunikationssysteme OpenScape Business X3W und OpenScape Business X5W sind ausschließlich für die Wandmontage freigegeben.

5.1.1 Wie Sie das Kommunikationssystem an einer Wand befestigen

Voraussetzungen

Die Voraussetzungen für die Auswahl des Montagestandorts wurden berücksichtigt (siehe [Voraussetzungen für die Installation](#) auf Seite 31).

Eine tragfähige Wand mit ausreichend Platz für die Montage des Kommunikationssystems und eventueller weiterer Komponenten (zum Beispiel ein Hauptverteiler) steht zur Verfügung.

Schritt für Schritt

- 1) Befestigen Sie die beiliegende Bohrschablone am gewünschten Montageort.
- 2) Bohren Sie drei Löcher.
- 3) Schieben Sie die Dübel in die Bohrlöcher und drehen Sie die Schrauben mit ca. 5 mm Überstand ein.

- 4) Hängen Sie das Kommunikationssystem an den Befestigungslöchern ein und richten Sie es aus.

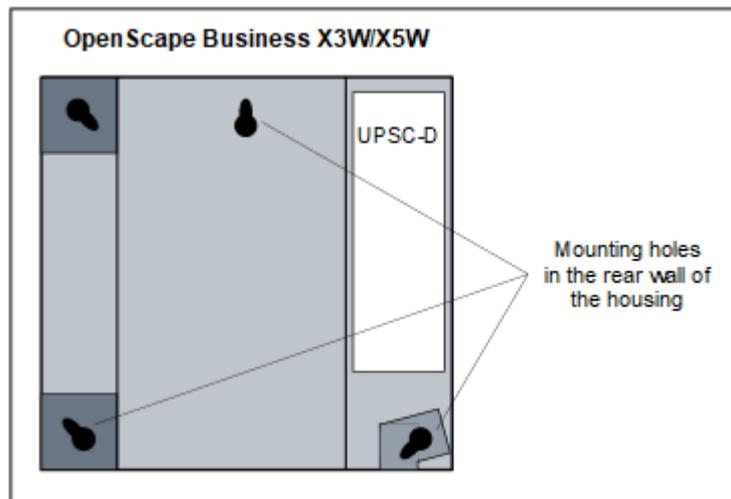


Abbildung 2: OpenScape Business X3W/X5W – Befestigungslöcher in der Gehäuserückwand

- 5) Drehen Sie die drei Schrauben fest.

5.2 Schutzerdung

Die Schutzerdung bietet eine sichere Verbindung zum Erdpotential, um Schutz vor gefährlich hohen Berührungsspannungen bei einer Fehlfunktion zu bieten.



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

- Schutzerden Sie die OpenScape Business X3W und OpenScape Business X5W Kommunikationssysteme und möglichst alle verwendeten Hauptverteiler durch separate Schutzleiter. Schließen Sie Ihr Kommunikationssystem und Ihren Hauptverteiler an den Schutzleiter an, bevor Sie das System in Betrieb nehmen und Telefone und Leitungen anschließen.
- Achten Sie darauf, dass die verlegten Schutzleiter geschützt und zugentlastet sind.



Achtung:

Montage der Schutzerdungsklemme

Bei Migration von HiPath 3350/3550 zu OpenScape Business X3W/X5W muss die Schutzerdungsklemme installiert werden, wie in [Abb: Montage der Schutzerdungsklemme](#) dargestellt.

Danach muss der Schutzerdungsleiter angeschlossen werden, wie in [Schutzerden des Hauptverteilers MDFU](#) dargestellt.

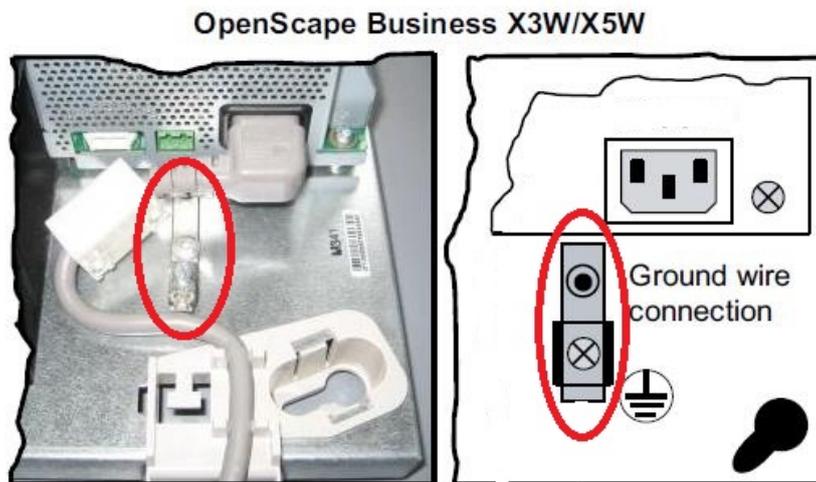


Abbildung 3: Montage der Schutzerdungsklemme

5.2.1 So nehmen Sie für Schutzerdung des Hauptverteilers MDFU vor

Voraussetzungen

Ein niederohmiger Masseanschluss ist vorhanden.



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.



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

- Schutzerden Sie die OpenScape Business X3W und OpenScape Business X5W Kommunikationssysteme und möglichst alle verwendeten Hauptverteiler durch separate Schutzleiter. Schließen Sie Ihr Kommunikationssystem und Ihren Hauptverteiler an den Schutzleiter an, bevor Sie das System in Betrieb nehmen und Telefone und Leitungen anschließen.
- Achten Sie darauf, dass die verlegten Schutzleiter geschützt und zugentlastet sind.

Die Erdung des Kommunikationssystems und des externen Hauptverteilers muss von einem Erdungspunkt in einer Sternkonfiguration erfolgen.

Die in IEC 60364, IEC 60950-1 und IEC 62368-1 angegebenen Ausführungsbestimmungen müssen bei der Installation eingehalten werden.

Anmerkung: Die aufgeführten Voraussetzungen gelten auch, wenn Sie einen Hauptverteiler eines anderen Herstellers statt dem MDFU verwenden.

Gehen Sie wie folgt vor, um die Schutzerdung sicherzustellen:

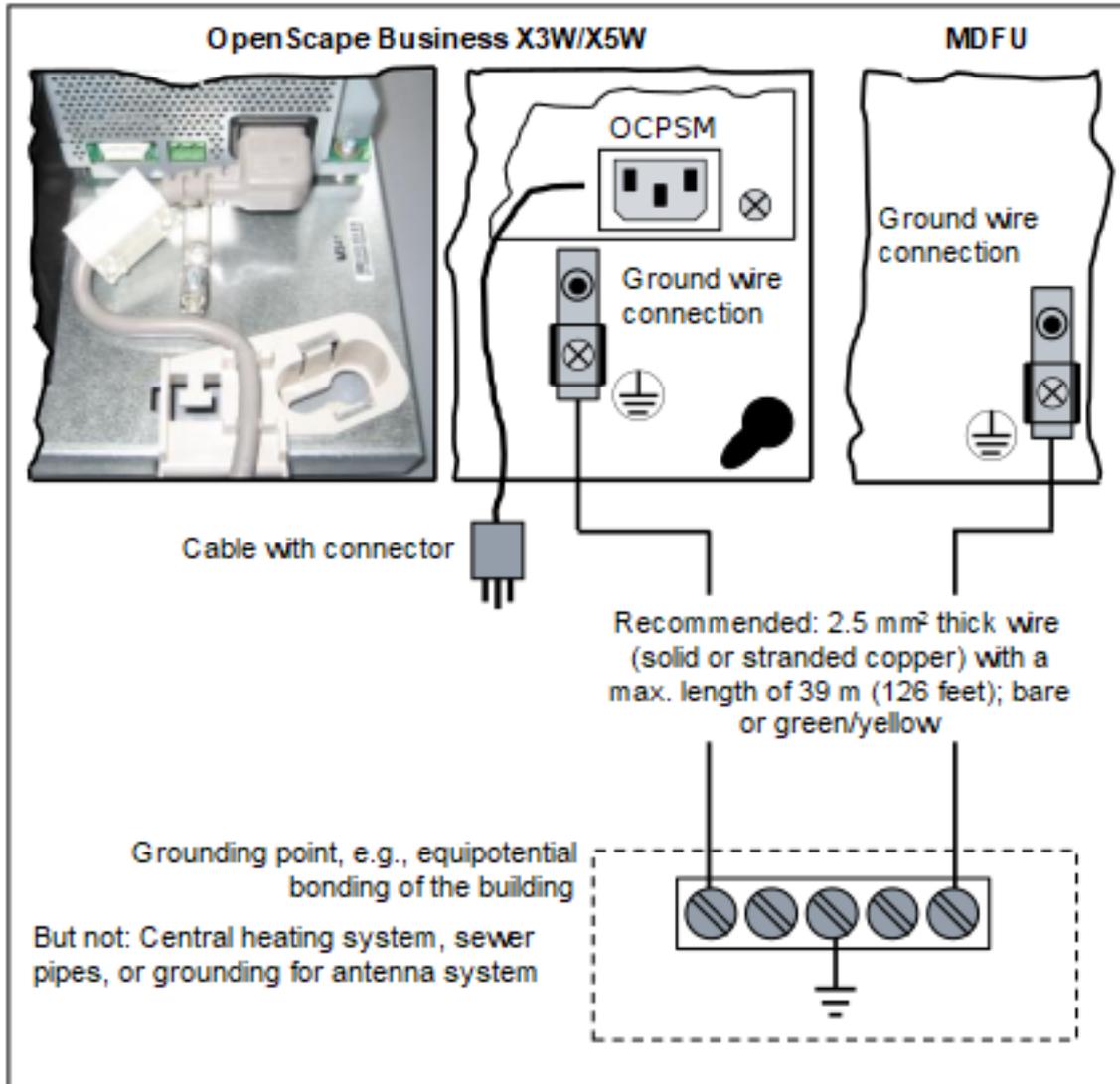
Schritt für Schritt

- 1) Schließen Sie einen separaten Schutzleiter an der Erdungsklemme des Kommunikationssystems an.
- 2) Sorgen Sie für die Zugentlastung des Schutzleiters, indem Sie ihn mit einem Kabelbinder am Kommunikationssystem befestigen.
- 3) Wenn ein MDFU vorhanden ist: Befestigen Sie einen separaten Schutzleiter an der Erdungsklemme des MDFU-Hauptverteilers.
- 4) Wenn ein MDFU vorhanden ist: Sorgen Sie für die Zugentlastung des Schutzleiters, indem Sie ihn mit einem Kabelbinder am Gehäuse des MDFU-Hauptverteilers befestigen.

5) Wählen Sie eine der folgenden Optionen:

- **Nicht für USA und Kanada - Potenzialausgleichsleiste**

Verbinden Sie den oder die separaten Schutzleiter mit dem Erdungspunkt (z. B. die Potenzialausgleichsleiste des Gebäudes), wie im Schaltdiagramm in der folgenden Abbildung dargestellt.

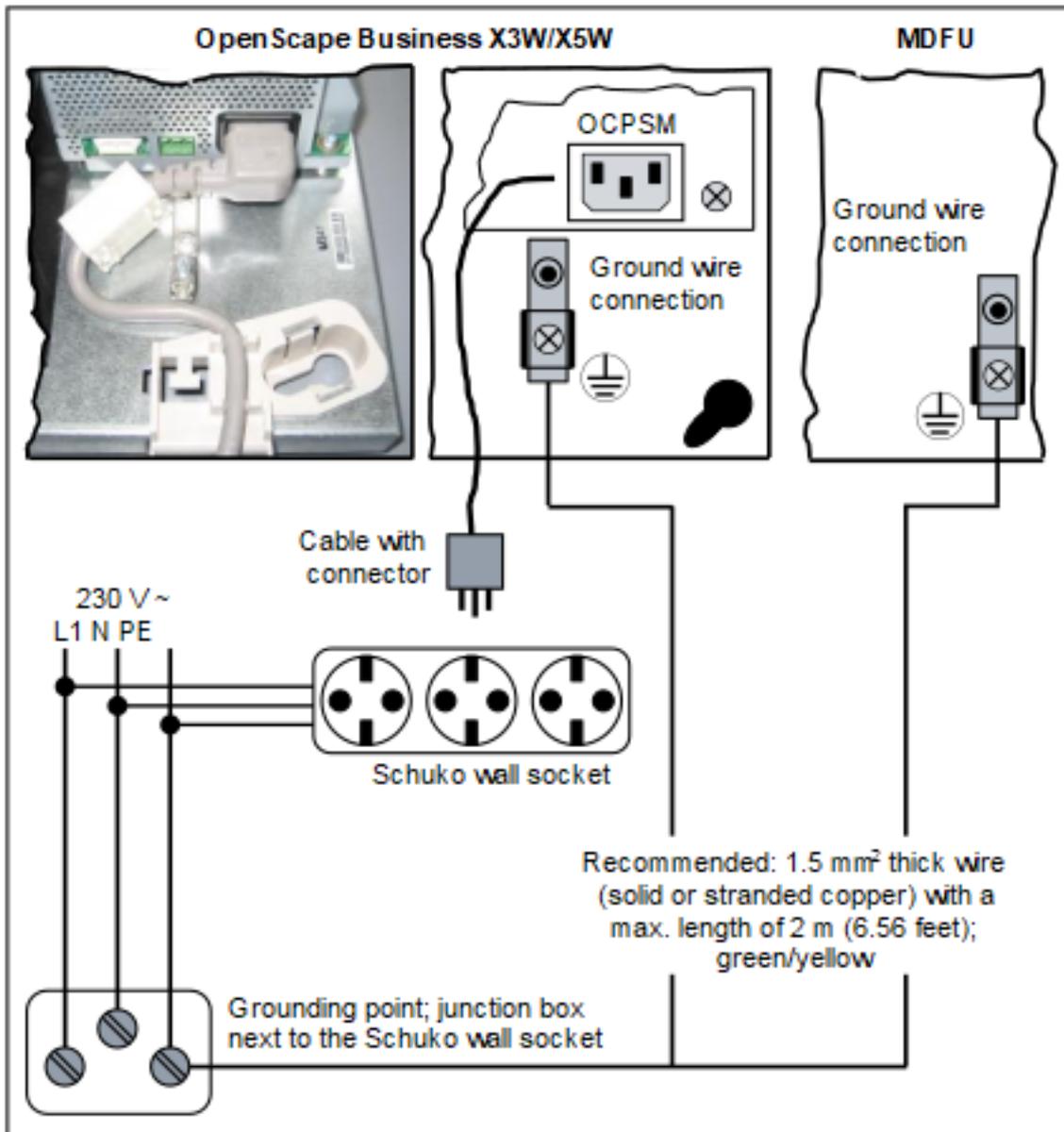


Achten Sie darauf, dass alle verlegten Schutzleiter geschützt und zugentlastet sind. Der minimale Leiterquerschnitt beträgt 12 AWG/2,5 mm². Ein Leiterquerschnitt von mindestens 10 AWG/4 mm² ist erforderlich, um die Auswirkungen externer Faktoren zu blockieren, wenn der Schutzleiter nicht geschützt werden kann.

- **Nicht für USA und Kanada - Anschluss an das Niederspannungsnetz**

Schließen Sie eine Anschlussdose in der Nähe der Schuko-Wandsteckdose, an die das Kommunikationssystem angeschlossen ist, an das Niederspannungsnetz an. Verwenden Sie einen separaten

Schutzleiter zum Einrichten einer festen Verbindung mit der Anschlussdose, wie im Schaltdiagramm dargestellt.



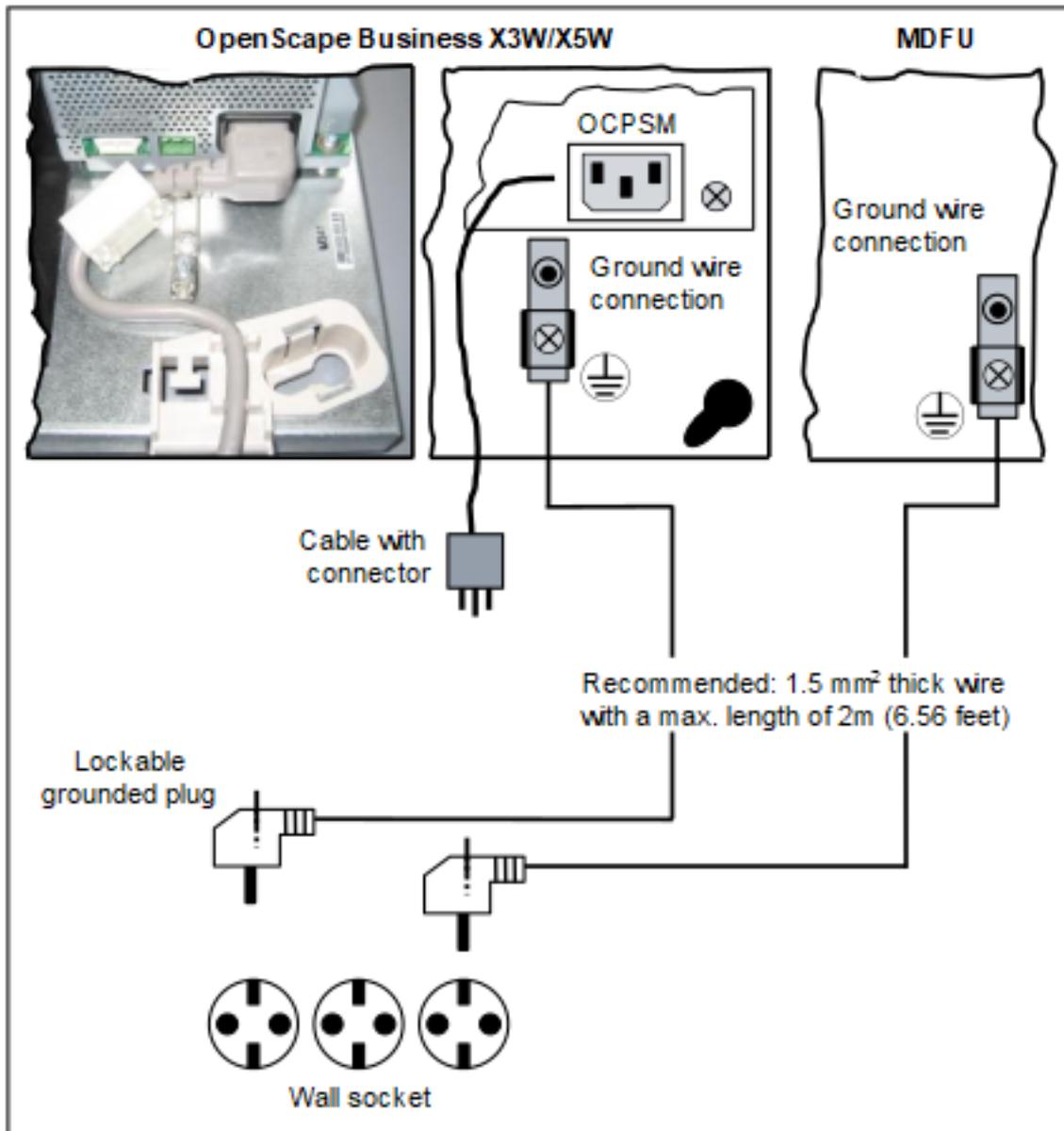
Achten Sie darauf, dass alle verlegten Schutzleiter geschützt und zugentlastet sind. Der minimale Leiterquerschnitt beträgt 16 AWG/1,5 mm².

- **Nicht für USA und Kanada - Verriegelbarer Schuko-Stecker für Niederspannungsnetz**

Setzen Sie den verriegelbaren Schuko-Stecker (spezieller Schuko mit festem Schutzleiter) in eine Wandsteckdose des Niederspannungsnetzes ein und verriegeln Sie den Stecker. Verwenden Sie den am Stecker angeschlossenen Schutzleiter zum Einrichten einer festen Verbindung mit dem Kommunikationssystem, wie im Schaltdiagramm dargestellt.

Hardwareinstallation von OpenScape Business X3W/X5W

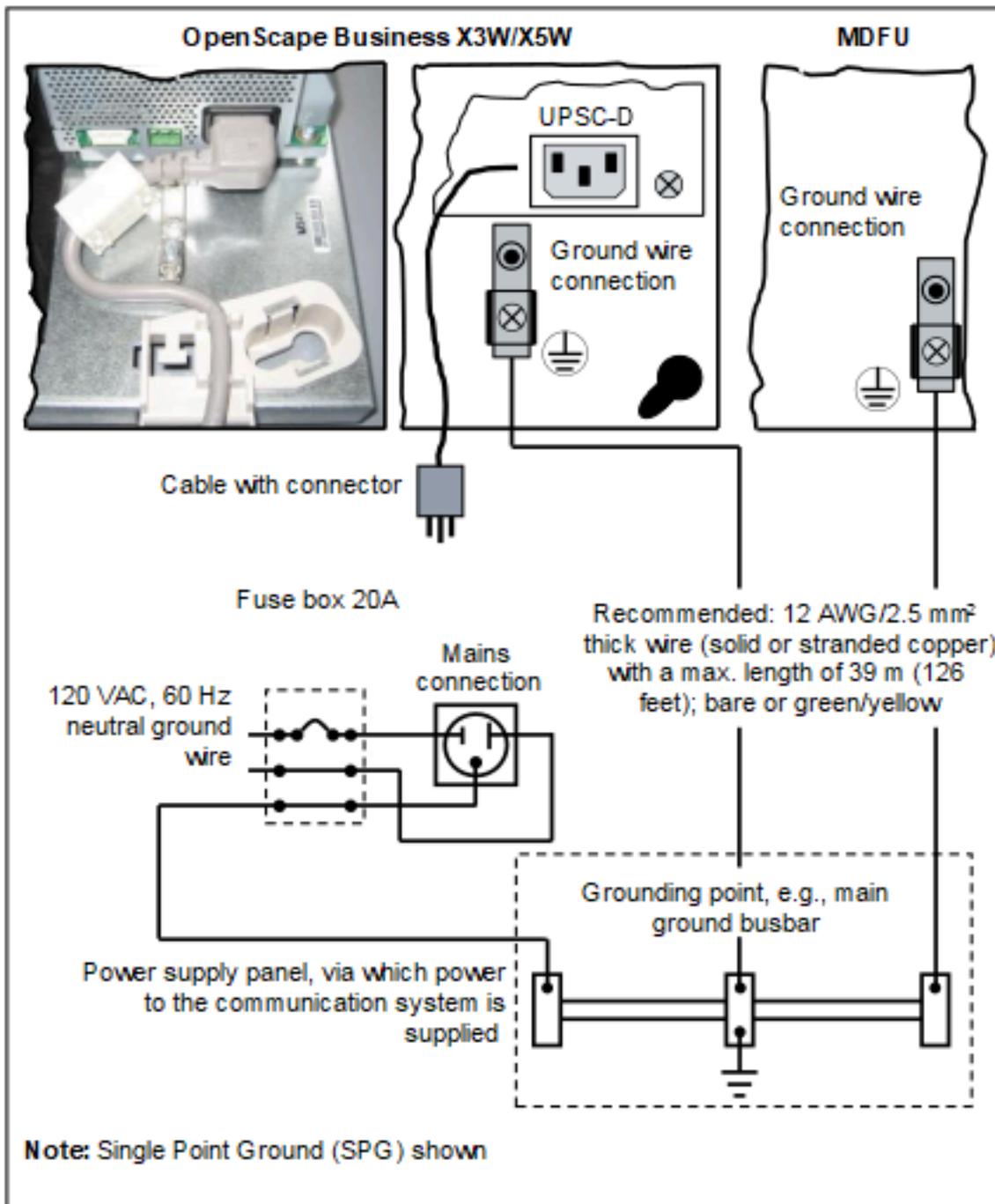
Verwenden Sie einen zweiten verriegelbaren Schuko-Stecker für einen möglicherweise vorhandenen MDFU.



Achten Sie darauf, dass alle verlegten Schutzleiter geschützt und zugentlastet sind. Der minimale Leiterquerschnitt beträgt 16 AWG/1,5 mm² für bis zu 2 m mindestens 12 AWG/2,5 mm² für 2 m und darüber.

- **Nur für USA und Kanada: Haupterdsammelschiene**

Verbinden Sie den oder die separaten Schutzleiter mit dem Erdungspunkt (z. B. Haupterdsammelschiene, Erdungsfeld), wie im Schalt diagramm in der folgenden Abbildung dargestellt.



Achten Sie darauf, dass alle verlegten Schutzleiter geschützt und zugentlastet sind. Der minimale Leiterquerschnitt beträgt 12 AWG/2,5 mm². Ein Leiterquerschnitt von mindestens 10 AWG/4 mm² ist erforderlich, um die Auswirkungen externer Faktoren zu blockieren, wenn der Schutzleiter nicht geschützt werden kann.

Hardwareinstallation von OpenScape Business X3W/X5W

Anschlusskabel für den direkten Anschluss von Telefonen, Amtsleitungen usw.

5.2.2 Wie Sie die Schutzerdung prüfen

Voraussetzungen

Das Kommunikationssystem ist **noch nicht** über das Netzanschlusskabel mit dem Niederspannungsnetz verbunden.

Die separate Schutzerdung für das Kommunikationssystem und für den eventuell verwendeten Hauptverteiler ist angeschlossen.

Führen Sie vor der Inbetriebnahme den folgenden Test durch, um die ordnungsgemäße Schutzerdung des Kommunikationssystems und des eventuell verwendeten Hauptverteilers sicherzustellen.

Schritt für Schritt

- 1) Prüfen Sie den Ohmschen Widerstand der separaten Schutzleiterverbindung zum Kommunikationssystem:

Die Messung erfolgt zwischen dem Schutzkontakt einer Schuko-Steckdose der Hausinstallation (am Anschlussort des Kommunikationssystems) und dem Gehäuse des Kommunikationssystems.

- 2) Falls ein Hauptverteiler verwendet wird, prüfen Sie den Ohmschen Widerstand der separaten Schutzleiterverbindung zum Hauptverteiler.

Die Messung erfolgt zwischen dem Schutzkontakt einer Schuko-Steckdose der Hausinstallation (am Anschlussort des Kommunikationssystems) und dem Gehäuse des Hauptverteilers.

Das Ergebnis (Sollwert) einer Messung muss wesentlich kleiner als 10 Ohm betragen.

Sollten Sie zu einem anderen Messergebnis kommen, beauftragen Sie einen qualifizierten Elektrotechniker. Dieser muss den Potentialausgleich der Hausinstallation prüfen und die Niederohmigkeit der Schutzleiterverbindung sicherstellen.

5.3 Anschlusskabel für den direkten Anschluss von Telefonen, Amtsleitungen usw.

Der Anschluss von Telefonen, Amtsleitungen usw. beim OpenScape Business Wandmodell erfolgt direkt an der Baugruppe.

CABLU C39195-A7001-B126

CABLU mit

- acht Wieland-Schraubklemmen für den direkten Anschluss an die Randstecker der Baugruppen der OpenScape Business Wandmodelle
- 8 x vier RJ45-Buchsen zum Anschluss von U_{P0/E}-Telefonen und analogen Telefonen und Geräten

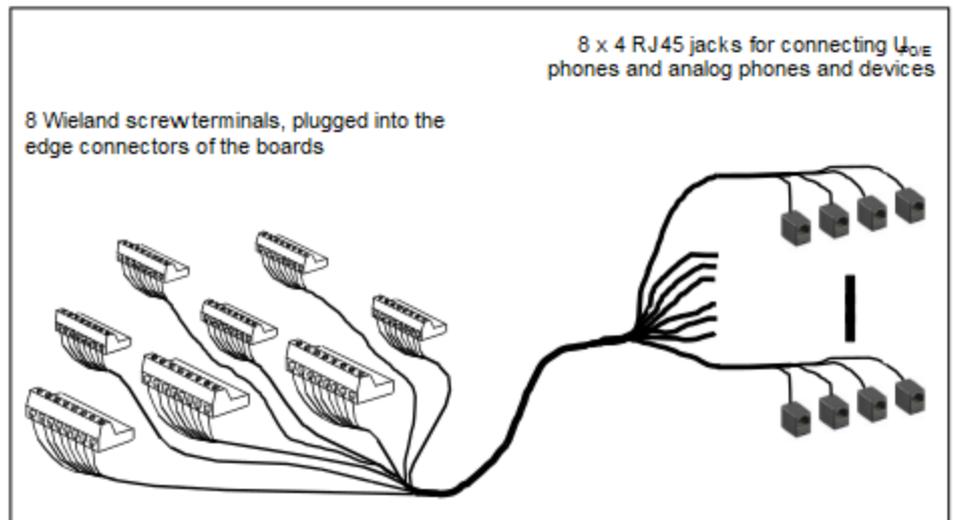


Abbildung 4: CABLU C39195-A7001-B126

Wieland-Schraubklemme

Bei Verwendung einzelner Wieland-Schraubklemmen müssen die Anschlussleitungen der Telefone, Amtsleitungen usw. einzeln angeschlossen werden.

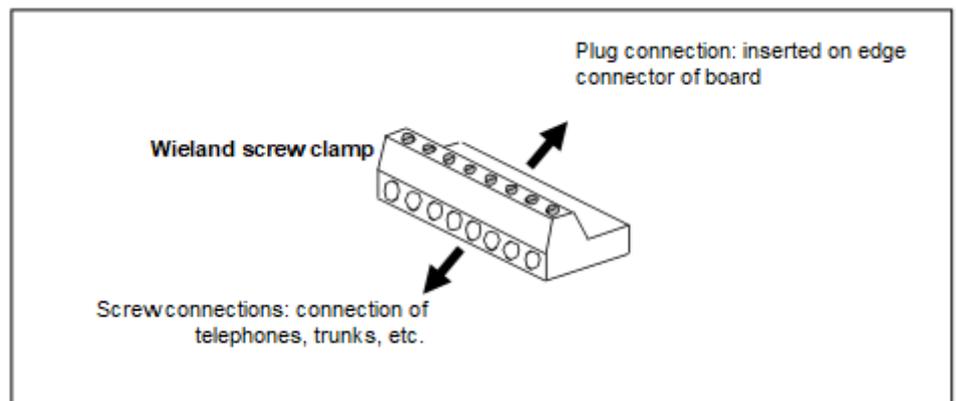


Abbildung 5: Wieland-Schraubklemme

5.4 Konfigurationshinweise

Die Konfigurationshinweise beinhalten Informationen über die Baugruppen-Steckplätze der Kommunikationssysteme OpenScape Business X3W und OpenScape Business X5W.

5.4.1 Baugruppen-Steckplätze in OpenScape Business X3W

OpenScape Business X3W beinhaltet einen Baugruppenrahmen, der drei Steckplatzebenen für die Bestückung mit Baugruppen und Optionen zur Verfügung stellt.

- Steckplatzebene 1: Steckplätze für zwei Peripheriebaugruppen

- Steckplatzebene 2: Steckplatz für das Mainboard OCCM
- Steckplatzebene 3: Steckplätze für fünf Optionen

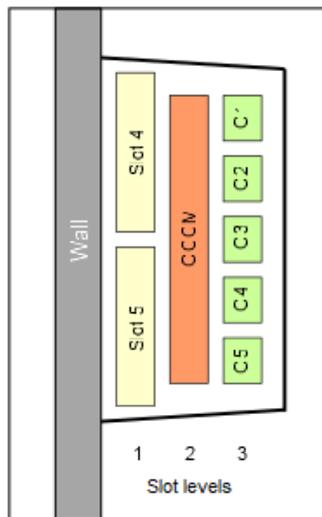


Abbildung 6: OpenScape Business X3W – Baugruppen-Steckplätze

5.4.2 Steckplätze in OpenScape Business X5W

OpenScape Business X5W beinhaltet einen Baugruppenrahmen mit sechs Steckplatzebenen.

Die Steckplatzebenen sind wie folgt ausgestattet:

- Steckplatzebenen 1 bis 3: Steckplätze für jeweils zwei Peripheriebaugruppen
- Steckplatzebene 4: Steckplatz für das Mainboard OCCM, OCCMA oder OCCMB
- Steckplatzebene 6: Steckplätze für fünf Optionen

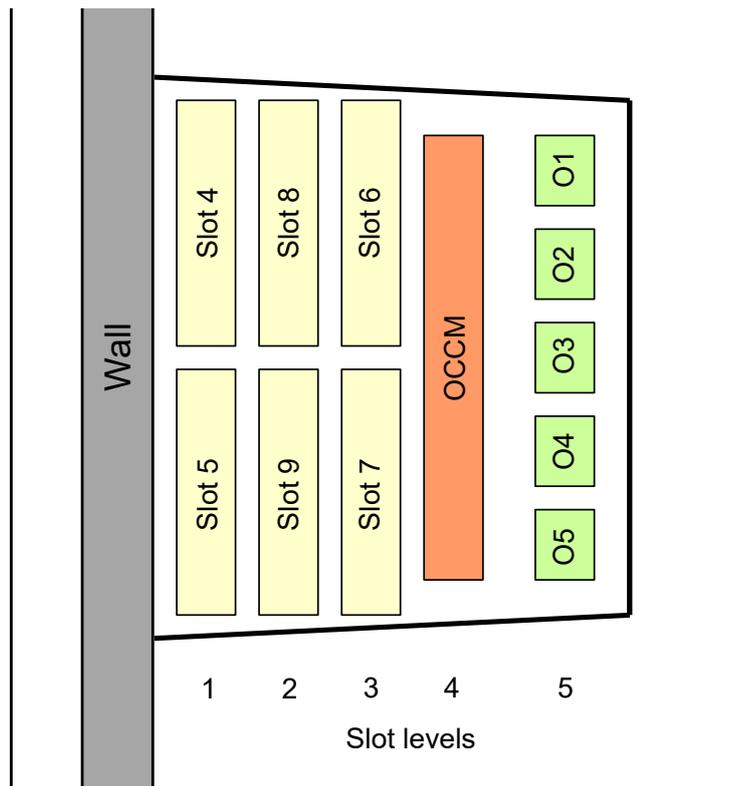


Abbildung 7: OpenScape Business X5W - Baugruppensteckplätze

Nur der neue Lüfterkit (L30251-U600-A985) kann in neuen Systemen verwendet werden. Vorhandenen Lüfterkits (L30251-U600-A918) können nicht angeschlossen werden.

Anmerkung: Vorhandene OpenScape Business Systeme müssen auf neue Backplanes aufgerüstet werden, falls ein UPSC-D/DR-Netzteil durch ein OCPSM ersetzt wird. Das entsprechende PSU Upgrade-Kit enthält alle nötigen Adapter und Kabel.

Bei der Migration von HiPath 33xx / 35xx zu OpenScape Business müssen die vorhandenen Backplanes nicht ersetzt werden, falls ein OCPSM-Netzteil statt der PSU mit dem entsprechenden PSU-Upgrade-Kit verwendet wird.

Die Steckplätze der neuen Backplane werden ab OpenScape Business V2 unterstützt. Systeme mit SW-Version V1 müssen auf SW-Version V2 aktualisiert werden, bevor die alte Backplane durch eine neue ersetzt wird.

Wichtig: (*) Mit neuen Backplanes wird Steckplatzebene 5 (Steckplatz 10) durch OpenScape Business X5W Wandsysteme nicht mehr bereitgestellt. Karten mit SIPAC-Anschlussleiste (SLMO24, SLC16N) können nicht in Kombination mit der neuen Backplane verwendet werden.

5.4.3 Baugruppeninstallation

5.4.3.1 Wie Sie eine Baugruppe stecken

Voraussetzungen

Die Gehäusekappe ist nicht montiert.

Ein freier Baugruppen-Steckplatz steht zur Verfügung.

Anmerkung: Grundsätzlich muss beim Arbeiten mit Baugruppen das Erdungsarmband getragen werden.

Die EGB-Schutzmaßnahmen sind zu beachten und zu befolgen (siehe [Warnhinweise: Hinweis](#) auf Seite 16)

Schritt für Schritt

- 1) Entfernen Sie die Stabilisatorkappe.
- 2) Schieben Sie die Baugruppe mit Hilfe der Führungsschienen bis zu Anschlag in den gewünschten Baugruppen-Steckplatz.
- 3) Montieren Sie die Stabilisatorkappe.

5.4.3.2 Wie Sie eine Baugruppe ziehen

Voraussetzungen

Die Gehäusekappe ist nicht montiert.

Anmerkung: Grundsätzlich muss beim Arbeiten mit Baugruppen das Erdungsarmband getragen werden.

Die EGB-Schutzmaßnahmen sind zu beachten und zu befolgen (siehe [Warnhinweise: Hinweis](#) auf Seite 16)

Schritt für Schritt

- 1) Entfernen Sie die Stabilisatorkappe.
- 2) Ziehen Sie die Baugruppe aus dem Baugruppenrahmen.
- 3) Montieren Sie die Stabilisatorkappe.

5.5 LAN- und WAN-Port

Die Kommunikationssysteme OpenScape Business X3W und OpenScape Business X5W bieten verschiedene Optionen für LAN- und WAN-Verbindungen .

Anmerkung: Um eine ausreichende elektromagnetische Abschirmung gemäß EN 55022 zu gewährleisten, muss der Kabelschirm jedes einzelnen LAN- und WAN-Kabels mit dem

Metallgehäuse des Kommunikationssystems leitend verbunden werden.

5.5.1 LAN- oder WAN-Anschluss durchführen

Voraussetzungen



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

Schutzerden Sie Ihr Kommunikationssystem und alle eventuell verwendeten Hauptverteiler vor Anschluss der Telefone und Leitungen durch separate Schutzleiter.



ACHTUNG:

Brandgefahr

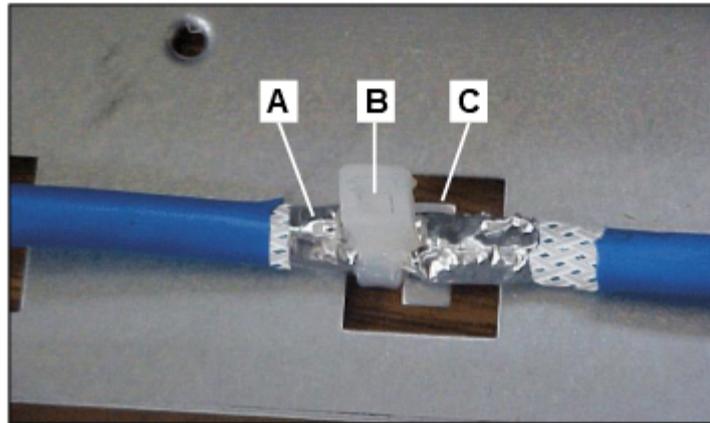
Um das Brandrisiko zu verringern, dürfen Sie nur Kommunikationsleitungen mit einem Leiterdurchmesser von mindestens 0,4 mm (AWG 26) oder größer verwenden. Empfohlen werden geschirmte Cat.5-Kabel (mehradrige Kabel bis 100 MHz für den Horizontal- und Steigbereich gemäß EN 50288). Diese sind mit einem Leiterdurchmesser von 0,4 mm bis 0,8 mm spezifiziert.

Mindestens eine freie LAN- oder WAN-Schnittstelle steht zur Verfügung (Mainboard OCCM oder Application Board OCAB).

Schritt für Schritt

- 1) Legen Sie die den Kabelschirm des LAN-/WAN-Kabels auf einer Länge von ca. 3 cm frei. Der freigelegte Kabelschirm muss sich in Reichweite einer T-Zunge des Gehäuses befinden.
- 2) Umwickeln Sie den freigelegten Kabelschirm des LAN-/WAN-Kabels mit leitfähigem Klebeband (mindestens 1,5fache Umwicklung).
- 3) Fixieren Sie den mit leitfähigem Klebeband umwickelten Kabelschirm [A] des LAN-/WAN-Kabels mittels eines Kabelbinders [B] so an einer T-Zunge

[C] des Gehäuses, dass eine dauerhaft leitende Verbindung zwischen Kabelschirm und Gehäuse gewährleistet ist.



- 4) Verbinden Sie den gewünschten LAN- oder WAN-Anschluss mit dem anzuschließenden Gerät (LAN-Switch, IP-Telefon, DSL-Modem usw.).

5.6 Amtsanschluss

Die Kommunikationssysteme OpenScape Business X3W und OpenScape Business X5W bieten verschiedene Möglichkeiten für den Amtsanschluss und damit für den Zugang zum öffentlichen Kommunikationsnetz.

Wählen Sie den oder die für Ihr Kommunikationssystem erforderlichen Amtsanschlüsse unter folgenden Möglichkeiten aus:

- ISDN-Anlagenanschluss und ISDN-Mehrgeräteanschluss über S_0 -Schnittstelle (nicht für USA, Kanada)
- Nur für OpenScape Business X5W: ISDN-Primärmultiplexanschluss über S_{2M} -Schnittstelle (nicht für USA, Kanada)
- Nur für OpenScape Business X5W: ISDN-Primärmultiplexanschluss über T1-Schnittstelle (nur für USA, Kanada)
- Nur für OpenScape Business X5W: Amtsanschluss mit CAS-Protokoll über CAS-Schnittstelle (nur für ausgewählte Länder)
- Analoger Amtsanschluss

5.6.1 Nicht für USA, Kanada: Wie Sie einen ISDN-Anlagen- oder ISDN-Mehrgeräteanschluss über eine S_0 -Schnittstelle durchführen

Voraussetzungen



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

Schutzerden Sie Ihr Kommunikationssystem und alle eventuell verwendeten Hauptverteiler vor Anschluss der Telefone und Leitungen durch separate Schutzleiter.



ACHTUNG:

Brandgefahr

Um das Brandrisiko zu verringern, dürfen Sie nur Kommunikationsleitungen mit einem Leiterdurchmesser von mindestens 0,4 mm (AWG 26) oder größer verwenden.

Mindestens eine freie S₀-Schnittstelle steht zur Verfügung (Mainboard OCCM oder Peripheriebaugruppe STLSX2, STLSX4, STLS2, STLS4).

Die verwendete S₀-Schnittstelle muss bei der Inbetriebnahme als ISDN-Anlagen- oder ISDN-Mehrgeräteanschluss konfiguriert werden.

Ein ISDN-Anlagen- oder ISDN-Mehrgeräteanschluss steht zur Verfügung.

Schritt für Schritt

Verbinden Sie den gewünschten S₀-Anschluss mit dem NTBA des ISDN-Anlagen- oder ISDN-Mehrgeräteanschlusses.

Wählen Sie dazu eine der folgenden Möglichkeiten:

- Wenn der Anschluss über den externen Hauptverteiler MDFU erfolgen soll, schließen Sie das Verbindungskabel zum NTBA an der gewünschten Trennleiste/Rangierleiste im MDFU an.
- Wenn der Anschluss direkt am Kommunikationssystem, das heißt über ein CABLU mit Wieland-Schraubklemmen erfolgen soll, stecken Sie das Verbindungskabel zum NTBA in die gewünschte RJ45-Buchse des CABLUS.

5.6.2 Nicht für USA, Kanada: Wie Sie einen ISDN-Primärmultiplexanschluss über eine S_{2M}-Schnittstelle durchführen (nur für OpenScape Business X5W)

Voraussetzungen



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

Schutzerden Sie Ihr Kommunikationssystem und alle eventuell verwendeten Hauptverteiler vor Anschluss der Telefone und Leitungen durch separate Schutzleiter.



ACHTUNG:

Brandgefahr

Um das Brandrisiko zu verringern, dürfen Sie nur Kommunikationsleitungen mit einem Leiterdurchmesser von mindestens 0,4 mm (AWG 26) oder größer verwenden.

OpenScape Business X5W ist mit einer Baugruppe TS2N bestückt.

Ein ISDN-Primärmultiplexanschluss steht zur Verfügung.

Schritt für Schritt

Verbinden Sie die S_{2M}-Schnittstelle mit dem NTPM des ISDN-Primärmultiplexanschlusses.

Wählen Sie dazu eine der folgenden Möglichkeiten:

- Wenn Sie eine symmetrische Leitung (120 Ohm) verwenden, erfolgt der Anschluss über Randstecker X2 der Baugruppe TS2N. Stecken Sie eine Wieland-Schraubklemme auf den Randstecker und schließen Sie das Verbindungskabel zum NTPM an.
- Wenn Sie eine Western-Leitung (Patch-Kabel) verwenden, erfolgt der Anschluss über RJ45-Buchse X5 der Baugruppe TS2N. Stecken Sie das Verbindungskabel zum NTPM in die RJ45-Buchse.

5.6.3 Nur für USA, Kanada: Wie Sie einen ISDN-Primärmultiplexanschluss über eine T1-Schnittstelle durchführen (nur für OpenScape Business X5W)

Voraussetzungen



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

Schutzerden Sie Ihr Kommunikationssystem und alle eventuell verwendeten Hauptverteiler vor Anschluss der Telefone und Leitungen durch separate Schutzleiter.



ACHTUNG:

Brandgefahr

Um das Brandrisiko zu verringern, dürfen Sie nur Kommunikationsleitungen mit einem Leiterdurchmesser von mindestens 0,4 mm (AWG 26) oder größer verwenden.

OpenScape Business X5W ist mit einer Baugruppe TST1 bestückt.

Eine Channel Service Unit (CSU) steht zur Verfügung, die nach FCC Part 68 zugelassen ist und die ANSI-Vorschrift T1.403 erfüllt. Die T1-Schnittstelle darf nicht direkt mit dem PSTN (Public Switched Telephone Network) verbunden werden. Es ist erforderlich, eine CSU zwischen Kommunikationssystem und digitalem Amtsanschluss zu schalten. Durch die CSU erhält OpenScape Business X5W folgende Merkmale: Isolierung und Überspannungsschutz des Kommunikationssystems, Diagnosemöglichkeiten im Fehlerfall (zum Beispiel Signal Loop Back, Einfügen von Testsignalen und Testmustern), Einpegeln des Ausgangssignals entsprechend den vom Netzanbieter vorgeschriebenen Leitungslängen. Eine CSU ist kein Lieferbestandteil des Kommunikationssystems OpenScape Business X5W.

Ein ISDN-Primärmultiplexanschluss steht zur Verfügung.

Schritt für Schritt

Verbinden Sie die T1-Schnittstelle mit der Channel Service Unit (CSU).

Der Anschluss erfolgt über Randstecker X2 der Baugruppe TST1. Stecken Sie eine Wieland-Schraubklemme auf den Randstecker und schließen Sie das Verbindungskabel zur CSU an.

5.6.4 Nur für ausgewählte Länder: Wie Sie einen Amtsanschluss über eine E1-CAS-Schnittstelle durchführen (nur für OpenScape Business X5W)

Voraussetzungen



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

Schutzerden Sie Ihr Kommunikationssystem und alle eventuell verwendeten Hauptverteiler vor Anschluss der Telefone und Leitungen durch separate Schutzleiter.



ACHTUNG:

Brandgefahr

Um das Brandrisiko zu verringern, dürfen Sie nur Kommunikationsleitungen mit einem Leiterdurchmesser von mindestens 0,4 mm (AWG 26) oder größer verwenden.

OpenScape Business X5W ist mit einer Baugruppe TCAS-2 bestückt.

Ein Amtsanschluss mit CAS-Protokoll steht zur Verfügung.

Schritt für Schritt

Verbinden Sie die gewünschte CAS-Schnittstelle der Baugruppe TCAS-2 mit dem NT des Amtsanschlusses.

5.6.5 Wie Sie einen analogen Amtsanschluss durchführen

Voraussetzungen



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

Schutzerden Sie Ihr Kommunikationssystem und alle eventuell verwendeten Hauptverteiler vor Anschluss der Telefone und Leitungen durch separate Schutzleiter.



ACHTUNG:

Brandgefahr

Hardwareinstallation von OpenScape Business X3W/X5W

Anschluss von Telefonen und Geräten

Um das Brandrisiko zu verringern, dürfen Sie nur Kommunikationsleitungen mit einem Leiterdurchmesser von mindestens 0,4 mm (AWG 26) oder größer verwenden.

Anmerkung:

Brandgefahr durch Überspannung

Bei Leitungslängen über 500 m und bei Leitungen, die das Gebäude verlassen, müssen die Baugruppen TLANI2, TLANI4 und TLANI8 durch einen externen Blitzschutz geschützt werden.

Ein solcher Blitzschutz wird als zusätzlicher Primärschutz bezeichnet. Der zusätzliche Primärschutz wird durch den 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.

Das Kommunikationssystem ist mit mindestens einer Baugruppe TLANI2, TLANI4 oder TLANI8 bestückt.

Nur für USA, Kanada: Ein Sicherungselement gemäß UL 497A oder CSA C22.2 No. 226 steht zur Verfügung. Die Installationsvorschriften erfordern, dass der Anschluss der analogen Amtsleitungen über Sicherungselemente gemäß UL 497A oder CSA C22.2 No. 226 erfolgen muss.

Ein analoger Amtsanschluss mit HKZ (Hauptanschlusskennzeichen)-Signalisierungsverfahren (Ground Start oder Loop Start) steht zur Verfügung.

Schritt für Schritt

Verbinden Sie den gewünschten a/b-Anschluss der gewünschten Baugruppe mit der TAE-Anschlussdose des analogen Amtsanschlusses.

Wählen Sie dazu eine der folgenden Möglichkeiten:

- Wenn der Anschluss über den externen Hauptverteiler MDFU erfolgen soll, schließen Sie das Verbindungskabel zur TAE-Anschlussdose an der gewünschten Trennleiste/Rangierleiste im MDFU an.
- Wenn der Anschluss direkt am Kommunikationssystem, das heißt über ein CABLU mit Wieland-Schraubklemmen erfolgen soll, stecken Sie das Verbindungskabel zur TAE-Anschlussdose in die gewünschte RJ45-Buchse des CABLUS.

5.7 Anschluss von Telefonen und Geräten

Die OpenScape Business Wall-Modelle bieten verschiedene Optionen für den Anschluss von Telefonen und Geräten.

Sie können den oder die erforderlichen Anschlüsse für Ihr Kommunikationssystem aus den folgenden Optionen wählen:

- Direkter Anschluss von ISDN-Telefonen (nicht für USA und Kanada)
- Anschluss von ISDN-Telefonen über den S₀-Bus (nicht für USA und Kanada)
- Anschluss von U_{P0/E}-Telefonen

- Anschluss von analogen Telefonen und Geräten

Anmerkung: An eine a/b-Schnittstelle kann nur ein analoges Gerät angeschlossen werden.

5.7.1 Nicht für USA, Kanada: Wie Sie ISDN-Telefone direkt anschließen

Voraussetzungen



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

Schutzerden Sie Ihr Kommunikationssystem und alle eventuell verwendeten Hauptverteiler vor Anschluss der Telefone und Leitungen durch separate Schutzleiter.



ACHTUNG:

Brandgefahr

Um das Brandrisiko zu verringern, dürfen Sie nur Kommunikationsleitungen mit einem Leiterdurchmesser von mindestens 0,4 mm (AWG 26) oder größer verwenden.

Anmerkung:

Brandgefahr durch Überspannung

Nur für die für den Teilnehmeranschluss verwendeten Schnittstellen: Bei Leitungslängen über 500 m und bei Leitungen, die das Gebäude verlassen, müssen die Baugruppen OCCM, STLSX2, STLSX4, STLS2 und STLS4 durch einen externen Blitzschutz geschützt werden.

Ein solcher Blitzschutz wird als zusätzlicher Primärschutz bezeichnet. Der zusätzliche Primärschutz wird durch den 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.

Mindestens eine freie S₀-Schnittstelle steht zur Verfügung (Mainboard OCCM oder Peripheriebaugruppe STLSX2, STLSX4, STLS2, STLS4).

Die verwendeten S₀-Schnittstellen müssen bei der Inbetriebnahme als interner S₀-Anschluss konfiguriert werden.

Die anzuschließenden ISDN-Telefone müssen über eine eigene Speisung verfügen, zum Beispiel über ein Steckernetzgerät. Eine Speisung über die S₀-Schnittstellen der Baugruppen OCCM, STLSX2, STLSX4, STLS2 und STLS4 ist nicht möglich.

Schritt für Schritt

1) Verbinden Sie den gewünschten S₀-Anschluss mit ISDN-Telefon.

Wählen Sie dazu eine der folgenden Möglichkeiten:

- Wenn der Anschluss über den externen Hauptverteiler MDFU erfolgen soll, schließen Sie das Verbindungskabel zum ISDN-Telefon an der gewünschten Trennleiste/Rangierleiste im MDFU an.
- Wenn der Anschluss direkt am Kommunikationssystem, das heißt über ein CABLU mit Wieland-Schraubklemmen erfolgen soll, stecken Sie das Verbindungskabel zum ISDN-Telefon in die gewünschte RJ45-Buchse des CABLUS.

Tipp:

Beachten Sie die Angaben in der Installationsanleitung des anzuschließenden Telefons.

2) Falls gewünscht, verbinden Sie weitere ISDN-Telefone auf die gleiche Weise mit dem Kommunikationssystem.

5.7.2 Nicht für USA, Kanada: Wie Sie ISDN-Telefone über den S₀-Bus anschließen

Voraussetzungen



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

Schutzerden Sie Ihr Kommunikationssystem und alle eventuell verwendeten Hauptverteiler vor Anschluss der Telefone und Leitungen durch separate Schutzleiter.



ACHTUNG:

Brandgefahr

Um das Brandrisiko zu verringern, dürfen Sie nur Kommunikationsleitungen mit einem Leiterdurchmesser von mindestens 0,4 mm (AWG 26) oder größer verwenden.

Anmerkung:

Brandgefahr durch Überspannung

Nur für die für den Teilnehmeranschluss verwendeten Schnittstellen: Bei Leitungslängen über 500 m und bei Leitungen, die das Gebäude verlassen, müssen die Baugruppen OCCM, STLSX2, STLSX4, STLS2 und STLS4 durch einen externen Blitzschutz geschützt werden.

Ein solcher Blitzschutz wird als zusätzlicher Primärschutz bezeichnet. Der zusätzliche Primärschutz wird durch den

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.

Mindestens eine freie S₀-Schnittstelle steht zur Verfügung (Mainboard OCCM oder Peripheriebaugruppe STLSX2, STLSX4, STLS2, STLS4).

Die verwendeten S₀-Schnittstellen müssen bei der Inbetriebnahme als interner S₀-Anschluss konfiguriert werden.

Die anzuschließenden ISDN-Telefone müssen über eine eigene Speisung verfügen, zum Beispiel über ein Steckernetzgerät. Eine Speisung über die S₀-Schnittstellen der Baugruppen OCCM, STLSX2, STLSX4, STLS2 und STLS4 ist nicht möglich.

Jedem einzelnen ISDN-Telefon (ISDN-Teilnehmer) muss eine eindeutige Multiple Subscriber Number MSN zugeordnet werden. Diese Zuordnung ist im Konfigurationsmenü des ISDN-Teilnehmers durchzuführen.

Schritt für Schritt

- 1) Verbinden Sie den gewünschten S₀-Anschluss mit der Mini-Western-Durchgangsdose des S₀-Busses.

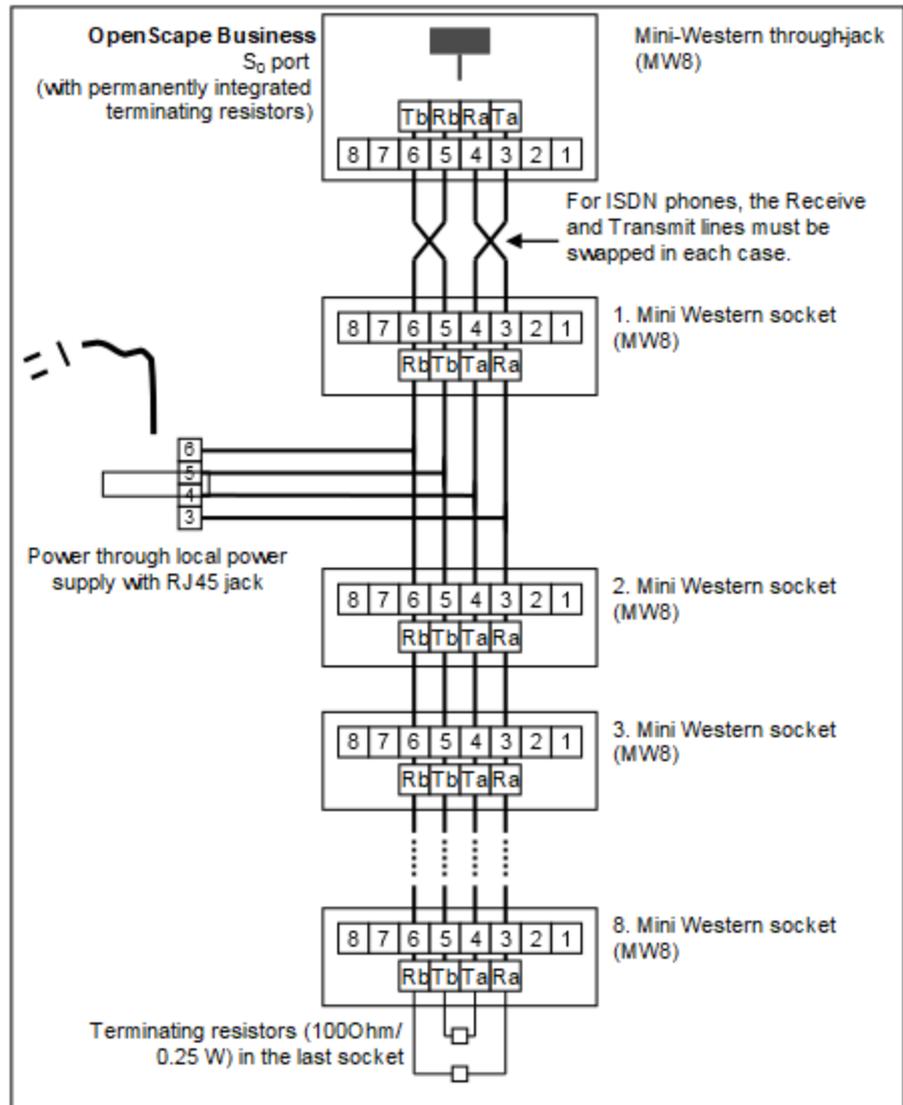
Wählen Sie dazu eine der folgenden Möglichkeiten:

- Wenn der Anschluss über den externen Hauptverteiler MDFU erfolgen soll, schließen Sie das Verbindungskabel zur Mini-Western-Durchgangsdose des S₀-Busses an der gewünschten Trennleiste/Rangierleiste im MDFU an.
- Wenn der Anschluss direkt am Kommunikationssystem, das heißt über ein CABLU mit Wieland-Schraubklemmen erfolgen soll, stecken Sie das Verbindungskabel zur Mini-Western-Durchgangsdose des S₀-Busses in die gewünschte RJ45-Buchse des CABLUS.

Tipp:

Beachten Sie die Angaben in der Installationsanleitung des anzuschließenden Telefons.

2) Führen Sie weitere Verdrahtung wie im folgenden Bild gezeigt durch.



- 3) Montieren Sie Abschlusswiderstände (100 Ohm/0,25 W) in der letzten Anschlussdose des S₀-Busses.
- 4) Stellen Sie sicher, dass nur an den beiden Enden des S₀-Busses Abschlusswiderstände vorhanden sind. Die weiteren Anschlussdosen des S₀-Busses benötigen keine Abschlusswiderstände.

Tipp:

Da Abschlusswiderstände in OpenScape Business X3W und OpenScape Business X5W bereits fest integriert sind, bildet das Kommunikationssystem das eine Ende eines S₀-Busses.

Tipp:

Beachten Sie die Angaben in der Installationsanleitung des anzuschließenden Telefons.

5.7.3 Wie Sie U_{P0/E}-Telefone anschließen

Voraussetzungen



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen
Schutzerden Sie Ihr Kommunikationssystem und alle eventuell verwendeten Hauptverteiler vor Anschluss der Telefone und Leitungen durch separate Schutzleiter.



ACHTUNG:

Brandgefahr

Um das Brandrisiko zu verringern, dürfen Sie nur Kommunikationsleitungen mit einem Leiterdurchmesser von mindestens 0,4 mm (AWG 26) oder größer verwenden.

Anmerkung:

Brandgefahr durch Überspannung

Bei Leitungslängen über 500 m und bei Leitungen, die das Gebäude verlassen, müssen die Baugruppen OCCM, SLU8, SLMO8 und SLMO24 durch einen externen Blitzschutz geschützt werden.

Ein solcher Blitzschutz wird als zusätzlicher Primärschutz bezeichnet. Der zusätzliche Primärschutz wird durch den 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.

Mindestens eine freie U_{P0/E}-Schnittstelle steht zur Verfügung (Mainboard OCCM oder Peripheriebaugruppe SLU8, SLMO8 (nur OpenScape Business X5W) oder SLMO24 (nur OpenScape Business X5W)).

Schritt für Schritt

1) Verbinden Sie den gewünschten U_{P0/E}-Anschluss mit dem U_{P0/E}-Telefon.

Wählen Sie dazu eine der folgenden Möglichkeiten:

- Wenn der Anschluss über den externen Hauptverteiler MDFU erfolgen soll, schließen Sie das Verbindungskabel zum U_{P0/E}-Telefon an der gewünschten Trennleiste/Rangierleiste im MDFU an.
-

Tipp: Nur für OpenScape Business X5W:
Bei Verwendung von U_{P0/E}-Schnittstellen der Peripheriebaugruppen SLMO8 und SLMO24 ist

der Anschluss ausschließlich über einen externen Hauptverteiler möglich.

- Wenn der Anschluss direkt am Kommunikationssystem, das heißt über ein CABLU mit Wieland-Schraubklemmen erfolgen soll, stecken Sie das Verbindungskabel zum U_{P0/E}-Telefon in die gewünschte RJ45-Buchse des CABLUS.

Tipp:

Beachten Sie die Angaben in der Installationsanleitung des anzuschließenden Telefons.

- 2) Falls gewünscht, verbinden Sie weitere U_{P0/E}-Telefone auf die gleiche Weise mit dem Kommunikationssystem.

5.7.4 Wie Sie analoge Telefone und Geräte anschließen

Voraussetzungen**Achtung:**

Elektrischer Schlag durch Berühren spannungsführender Leitungen

Schutzerden Sie Ihr Kommunikationssystem und alle eventuell verwendeten Hauptverteiler vor Anschluss der Telefone und Leitungen durch separate Schutzleiter.

**ACHTUNG:**

Brandgefahr

Um das Brandrisiko zu verringern, dürfen Sie nur Kommunikationsleitungen mit einem Leiterdurchmesser von mindestens 0,4 mm (AWG 26) oder größer verwenden.

Anmerkung:

Brandgefahr durch Überspannung

Bei Leitungslängen über 500 m und bei Leitungen, die das Gebäude verlassen, müssen die Baugruppen OCCM, SLAD4, SLAD8, SLAD16, 4SLA, 8SLA, 16SLA, SLA16N und SLA24N durch einen externen Blitzschutz geschützt werden.

Ein solcher Blitzschutz wird als zusätzlicher Primärschutz bezeichnet. Der zusätzliche Primärschutz wird durch den 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.

Mindestens eine freie a/b-Schnittstelle steht zur Verfügung (Mainboard OCCM oder Peripheriebaugruppe SLAD4, SLAD8, SLAD16, 4SLA, 8SLA, 16SLA, SLA16N (nur OpenScape Business X5W) oder SLA24N (nur OpenScape Business X5W)).

Schritt für Schritt

- 1) Verbinden Sie den gewünschten a/b-Anschluss mit dem anzuschließenden analogen Telefon oder analogen Gerät (Fax, Modem, TFE-S usw.).

Wählen Sie dazu eine der folgenden Möglichkeiten:

- Wenn der Anschluss über den externen Hauptverteiler MDFU erfolgen soll, schließen Sie das Verbindungskabel zum analogen Telefon oder analogen Gerät an der gewünschten Trennleiste/Rangierleiste im MDFU an.

Tipp:

Nur für OpenScape Business X5W: Bei Verwendung von a/b-Schnittstellen der Peripheriebaugruppen SLA16N und SLA24N ist der Anschluss ausschließlich über einen externen Hauptverteiler möglich.

- Wenn der Anschluss direkt am Kommunikationssystem, das heißt über ein CABLU mit Wieland-Schraubklemmen erfolgen soll, stecken Sie das Verbindungskabel zum analogen Telefon oder analogen Gerät in die gewünschte RJ45-Buchse des CABLUS.

Tipp:

Beachten Sie die Angaben in der Installationsanleitung des anzuschließenden Telefons/Geräts.

- 2) Falls gewünscht, verbinden Sie weitere analoge Telefone oder Geräte auf die gleiche Weise mit dem Kommunikationssystem.

5.8 Störaussendungen

Um die von der EMV-Klasse B zulässigen Grenzwerte für Störaussendungen einzuhalten, müssen Ferrite an bestimmten Leitungen des Kommunikationssystems angebracht werden.

Netzkabel

Um Störaussendungen zu minimieren, muss das Netzkabel durch die Ferrithülse C39022-Z7000-C7 geführt werden, die im Lieferumfang der Zusatzausrüstung des Kommunikationssystems enthalten ist.

Peripheriekabel

Um Störaussendungen zu minimieren, müssen die Peripheriekabel mit Ferrithülsen ausgestattet sein. Hierfür sollten die fünf im Lieferumfang des Kommunikationssystems enthaltenen Ferrithülsen C39022-Z7000-C6 verwendet werden.

Die Ferrithülsen sollten möglichst innerhalb des Kabelkanals positioniert werden. Wenn dies durch die Anzahl der Leitungen nicht möglich ist, sollte die Ferrithülse direkt am Ausgang des Kabelkanals angebracht werden.

Wenn die Anzahl der mitgelieferten Ferrithülsen nicht für alle Verbindungskabel ausreicht, müssen zusätzliche Ferrithülsen bestellt werden: L30460-X1358-X umfasst fünf Ferrithülsen C39022-Z7000-C6.

- OpenScape Business X3W
 - OCCM, OCCMA und OCCMB (Mainboard)

Die Verbindungskabel aller $U_{P0/E-}$, a/b- und S_0 -Schnittstellen müssen mit der Ferrithülse C39022-Z7000-C6 ausgestattet sein.

Die Verbindungskabel müssen zweimal durch eine Ferrithülse geführt werden, also in einer Schleife. Pro Ferrithülse sind maximal drei Verbindungskabel zulässig.
 - Alle Module für Amts-, Quer- und Teilnehmerleitungen

Die Verbindungskabel für alle Schnittstellen müssen mit der Ferrithülse C39022-Z7000-C6 ausgestattet sein.

Die Verbindungskabel müssen zweimal durch eine Ferrithülse geführt werden, also in einer Schleife. Pro Ferrithülse sind maximal drei Verbindungskabel zulässig.
- OpenScape Business X5W
 - OCCM, OCCMA und OCCMB (Mainboard)

Die Verbindungskabel aller $U_{P0/E-}$, a/b- und S_0 -Schnittstellen müssen mit der Ferrithülse C39022-Z7000-C6 ausgestattet sein.

Die Verbindungskabel müssen zweimal durch eine Ferrithülse geführt werden, also in einer Schleife. Pro Ferrithülse sind maximal drei Verbindungskabel zulässig.
 - Alle Module für Amts-, Schnurlos-, Quer- und Teilnehmerleitungen

Die Verbindungskabel für alle Schnittstellen müssen mit der Ferrithülse C39022-Z7000-C6 ausgestattet sein.

Die Verbindungskabel müssen zweimal durch eine Ferrithülse geführt werden, also in einer Schleife. Pro Ferrithülse sind maximal drei Verbindungskabel zulässig.

5.8.1 Wie Sie einen Ferrit an der Netzanschlussleitung anbringen

Voraussetzungen



Achtung:

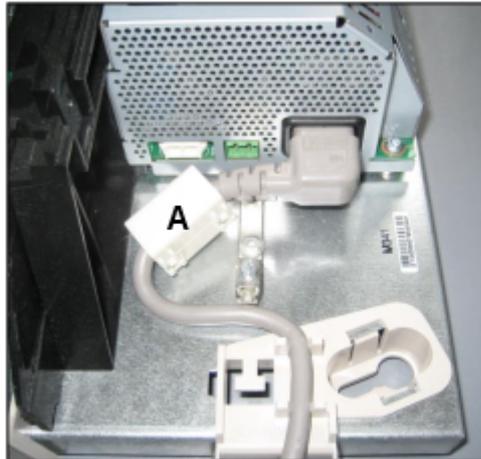
Elektrischer Schlag durch Berühren spannungsführender Leitungen

Schutzerden Sie Ihr Kommunikationssystem und alle eventuell verwendeten Hauptverteiler vor Inbetriebnahme durch separate Schutzleiter.

Die Gehäusekappe des Kommunikationssystems ist nicht montiert.

Schritt für Schritt

- 1) Führen Sie die Netzanschlussleitung durch den zum Lieferumfang des Kommunikationssystems gehörenden Klapp-Ferrit C39022-Z7000-C7.
- 2) Positionieren Sie den Klapp-Ferrit [A] wie im folgenden Bild gezeigt, um das Schließen der Gehäusekappe zu ermöglichen.



5.8.2 Wie Sie Ferrite an den Peripherie-Anschlussleitungen anbringen

Voraussetzungen



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen
Schutzerden Sie Ihr Kommunikationssystem und alle eventuell verwendeten Hauptverteiler vor Inbetriebnahme durch separate Schutzleiter.

Die Gehäusekappe des Kommunikationssystems ist nicht montiert.

Schritt für Schritt

Wählen Sie die Vorgehensweise anhand des Kommunikationssystems und der Baugruppe aus.

Hardwareinstallation von OpenScape Business X3W/X5W

Wenn		Dann
Kommunikationssystem	Baugruppe	
OpenScape Business X3W	Mainboard OCCM	<p>Führen Sie die Anschlussleitungen aller U_{P0/E^-}, a/b- und S_0-Schnittstellen zweifach, das heißt in einer Schlaufe durch einen Klapp-Ferrit C39022-Z7000-C6.</p> <p>Platzieren Sie die Klapp-Ferrite möglichst innerhalb des Kabelkanals. Ist dies aufgrund der Anzahl der Leitungen nicht möglich, bringen Sie die Klapp-Ferrite unmittelbar am Ausgang des Kabelkanals an.</p> <p>Maximal drei Anschlussleitungen pro Klapp-Ferrit sind zugelassen.</p>
	Alle Amts-, Querverkehr- und Teilnehmerbaugruppen	<p>Führen Sie die Anschlussleitungen aller Schnittstellen zweifach, das heißt in einer Schlaufe durch einen Klapp-Ferrit C39022-Z7000-C6.</p> <p>Platzieren Sie die Klapp-Ferrite möglichst innerhalb des Kabelkanals. Ist dies aufgrund der Anzahl der Leitungen nicht möglich, bringen Sie die Klapp-Ferrite unmittelbar am Ausgang des Kabelkanals an.</p> <p>Maximal drei Anschlussleitungen pro Klapp-Ferrit sind zugelassen.</p>
OpenScape Business X5W	Mainboard OCCM	<p>Führen Sie die Anschlussleitungen aller U_{P0/E^-}, a/b- und S_0-Schnittstellen zweifach, das heißt in einer Schlaufe durch einen Klapp-Ferrit C39022-Z7000-C6.</p> <p>Platzieren Sie die Klapp-Ferrite möglichst innerhalb des Kabelkanals. Ist dies aufgrund der Anzahl der Leitungen nicht möglich, bringen Sie die Klapp-Ferrite unmittelbar am Ausgang des Kabelkanals an.</p> <p>Maximal drei Anschlussleitungen pro Klapp-Ferrit sind zugelassen.</p>
	SLA16N SLC16N SLMO8	<p>Führen Sie das Anschlusskabel am SIPAC 1 SU-Stecker X8 der Backplane durch zwei Klapp-Ferrite C39022-Z7000-C6.</p> <p>Platzieren Sie die Klapp-Ferrite möglichst innerhalb des Gehäuses.</p>

Wenn		Dann
Kommunikationssystem	Baugruppe	
	SLA24N SLMO24	Führen Sie die beiden Anschlusskabel an den SIPAC 1 SU-Steckern X8 und X9 der Backplane durch jeweils zwei Klapp-Ferrite C39022-Z7000-C6. Platzieren Sie die Klapp-Ferrite möglichst innerhalb des Gehäuses.
	Alle weiteren Amts-, Cordless-, Querverkehr- und Teilnehmerbaugruppen	Führen Sie die Anschlussleitungen aller Schnittstellen zweifach, das heißt in einer Schlaufe durch einen Klapp-Ferrit C39022-Z7000-C6. Platzieren Sie die Klapp-Ferrite möglichst innerhalb des Kabelkanals. Ist dies aufgrund der Anzahl der Leitungen nicht möglich, bringen Sie die Klapp-Ferrite unmittelbar am Ausgang des Kabelkanals an. Maximal drei Anschlussleitungen pro Klapp-Ferrit sind zugelassen.

5.9 Abschließende Tätigkeiten

Zum Abschluss der Montage ist die SDHC-Karte zu stecken, eine Sichtkontrolle durchzuführen, die Gehäusekappe aufzusetzen und das System an das Stromnetz zu nehmen.

Anschließend kann das Kommunikationssystem mit dem OpenScape Business Assistant (WBM) in Betrieb genommen werden. Die Beschreibung dazu finden Sie in der Online-Hilfe des WBM oder in der Administrator Dokumentation im Kapitel "Erstinstallation OpenScape Business".

Anmerkung: Bei der Erstinbetriebnahme des Kommunikationssystems ist der Ladezustand des Akkus auf dem Mainboard nicht definiert. Um einen ausreichenden Ladezustand zu erreichen, muss das System mindestens 2 Tage am Stromnetz bleiben. Wird das System vom Stromnetz getrennt, kann es bei unzureichendem Ladezustand des Akkus vorkommen, dass die Activation Period wegen Zeitmanipulation gesperrt wird.

5.9.1 So setzen Sie die M.2 SSD oder die SDHC-Karte ein (System mit OCCM)

Die M.2 SSD oder die SDHC-Karte enthält die OpenScape Business Kommunikationssoftware und muss vor dem Starten des Kommunikationssystems eingebaut/eingesetzt werden.

Schritt für Schritt

- 1) Vergewissern Sie sich, dass der Schreibschutz der SDHC-Karte deaktiviert ist (Schalter Richtung Metallkontakte).
- 2) Stecken Sie die SDHC-Karte in den SDHC-Steckplatz des Mainboards, bis sie einrastet. Die Metallkontakte der SDHC-Karte müssen dabei Richtung Mainboard zeigen.

5.9.2 Wie Sie eine Sichtkontrolle durchführen

Vor Inbetriebnahme des Kommunikationssystems muss eine Sichtkontrolle der Hardware, der Verkabelung und der Spannungsversorgung durchgeführt werden.

Voraussetzungen



GEFAHR:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

Trennen Sie sämtliche Versorgungsstromkreise des Kommunikationssystems, bevor Sie mit der Sichtkontrolle beginnen:

- Schalten Sie Akkuspannung, Speisespannung (LUNA2) und Netzspannung einer eventuell angeschlossenen OpenScape Business Powerbox ab.
 - Ziehen Sie die Anschlussleitungen einer eventuell angeschlossenen OpenScape Business Powerbox.
 - Ziehen Sie die Anschlussleitungen eines eventuell angeschlossenen Akkupacks oder eventuell angeschlossener Akkus.
 - Ziehen Sie den Netzanschlussstecker des Kommunikationssystems.
-

Anmerkung:

Grundsätzlich muss beim Arbeiten mit Baugruppen das Erdungsarmband getragen werden.

Die EGB-Schutzmaßnahmen sind zu beachten und zu befolgen (siehe [Warnhinweise: Hinweis](#)).

Die Gehäusekappe des Kommunikationssystems ist nicht montiert.

Schritt für Schritt

- 1) Trennen Sie sämtliche Versorgungsstromkreise des Kommunikationssystems.
- 2) Prüfen Sie, ob das Kommunikationssystem spannungsfrei ist.
- 3) Prüfen Sie, ob die SDHC-Karte korrekt eingerastet ist. Der Schreibschutz der SDHC-Karte muss deaktiviert sein (Schalter Richtung Metallkontakte).
- 4) Prüfen Sie sämtliche Baugruppen auf festen Sitz.

Falls erforderlich, sorgen Sie für das korrekte Stecken der betroffenen Baugruppen (siehe [Wie Sie eine Baugruppe stecken](#)).

- 5) Prüfen Sie die korrekte Verlegung aller Anschluss- und Verbindungskabel. Sind beispielsweise Stolpergefahren vorhanden?

Falls erforderlich, sorgen Sie für eine korrekte Verlegung der Anschluss- und Verbindungskabel.

- 6) Prüfen Sie, ob ein separat geführter Schutzleiter am Schutzleiteranschluss des Kommunikationssystems angeschlossen ist.

Falls erforderlich, führen Sie die separate Schutzerdung des Kommunikationssystems durch (siehe [Wie Sie das Kommunikationssystem und den Hauptverteiler MDFU schutzerden](#)).

- 7) Prüfen Sie, ob eventuell verwendete Hauptverteiler ordnungsgemäß mit dem Schutzleiter verbunden sind.

Falls erforderlich, führen Sie die Schutzerdung aller Hauptverteiler durch (siehe [Wie Sie das Kommunikationssystem und den Hauptverteiler MDFU schutzerden](#)).

- 8) Prüfen Sie, ob die Nennspannung der Netzspannungsversorgung mit der Nennspannung des Kommunikationssystems (Typenschild) übereinstimmt.

Nächste Schritte

Verschließen Sie das Kommunikationssystem mit der Gehäusekappe (siehe [Wie Sie die Gehäusekappe aufsetzen](#)).

5.9.3 Wie Sie die Gehäusekappe aufsetzen

Schritt für Schritt

- 1) Setzen Sie die Gehäusekappe auf das Kommunikationssystem. Platzieren Sie dabei die beiden Halterungsstifte in die dafür vorgesehenen Löcher des Baugruppenrahmens.



ACHTUNG: Schnittwunden durch scharfkantiges Abschirmblech

Fassen Sie die Gehäusekappe nur von außen. Ansonsten können Schnittwunden durch das eventuell scharfkantige Abschirmblech an der Innenseite der Gehäusekappe hervorgerufen werden.



2) Sichern Sie die Gehäusekappe mit den beiden Befestigungsschrauben.

5.9.4 Wie Sie das System ans Stromnetz anschließen

Schritt für Schritt

Stecken Sie das Netzanschlusskabel in die Buchse der Stromversorgung. Das Kommunikationssystem fährt hoch.

Anmerkung: Lassen Sie das System mindestens 2 Tage am Stromnetz, damit der Akku des Mainboards einen ausreichenden Ladezustand erreicht. Bei unzureichendem Ladezustand kann es vorkommen, dass bei wiederholtem Hochfahren des Systems die Activation Period wegen Zeitmanipulation gesperrt wird.

6 Hardwareinstallation von OpenScape Business X3R/ X5R

Beschrieben ist die vorwiegend durchgeführte Standardmontage der Kommunikationssysteme OpenScape Business X3R und OpenScape Business X5R.

OpenScape Business X3R und OpenScape Business X5R sind Kommunikationssysteme im 19"-Rackgehäuse, die in einen 19"-Schrank montiert, frei aufgestellt (Tischbetrieb) oder an einer Wand montiert werden können.



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

- Arbeiten am geöffneten Gehäuse dürfen nur im spannungsfreien Zustand durchgeführt werden.
 - Prüfen Sie vor Beginn jeder Arbeit, ob alle Stromkreise spannungsfrei sind. Halten Sie es nie für selbstverständlich, dass mit Ausschalten einer Sicherung oder eines Hauptschalters alle Stromkreise auch zuverlässig unterbrochen sind.
-

6.1 Montagearten

Die Kommunikationssysteme OpenScape Business X3R und OpenScape Business X5R können in einen 19"-Schrank montiert, an einer Wand befestigt oder frei aufgestellt (Tischbetrieb) werden.

6.1.1 Wie Sie OpenScape Business X3R in einen 19"-Schrank montieren

Voraussetzungen

Die Voraussetzungen für die Auswahl des Montagestandorts wurden berücksichtigt (siehe [Voraussetzungen für die Installation](#) auf Seite 31).

Schrankspezifische Schrauben für die Befestigung der Haltewinkel am 19"-Schrank stehen zur Verfügung (sind vom Lieferanten des 19"-Schranks bereitzustellen).

Schritt für Schritt

- 1) Befestigen Sie die beiden zum Lieferumfang gehörenden Haltewinkel mit jeweils zwei der beiliegenden Schrauben an den Seiten des Kommunikationssystems.



Abbildung 8: OpenScape Business X3R – Haltewinkel

- 2) Heben Sie das Kommunikationssystem in den 19"-Schrank und befestigen Sie dieses anhand der beiden Haltewinkel [A] mit den dafür vorgesehenen Schrauben am 19"-Schrank.



6.1.2 Wie Sie OpenScape Business X5R in einen 19"-Schrank montieren

Voraussetzungen

Die Voraussetzungen für die Auswahl des Montagestandorts wurden berücksichtigt (siehe [Voraussetzungen für die Installation](#) auf Seite 31).

Schrankspezifische Schrauben für die Befestigung der Auflegewinkel und der Haltewinkel am 19"-Schränk stehen zur Verfügung (sind vom Lieferanten des 19"-Schranks bereitzustellen).

Schritt für Schritt

- 1) Befestigen Sie die beiden zum Lieferumfang gehörenden Haltewinkel mit jeweils zwei der beiliegenden Schrauben an den Seiten des Kommunikationssystems.



Abbildung 9: OpenScape Business X5R – Haltewinkel

- 2) Montieren Sie einen rechten und einen linken Auflegewinkel (Teil des Montagesatzes für die 19"-Schränkmontage (C39165-A7027-D1)) mit den dafür vorgesehenen Schrauben am 19"-Schränk.



Abbildung 10: OpenScape Business X5R – Auflegewinkel

- 3) Heben Sie das Kommunikationssystem in den 19"-Schränk und setzen Sie dieses auf den beiden Auflegewinkeln [A] ab. Schieben Sie das Kommunikationssystem soweit in den 19"-Schränk, bis die beiden Haltewinkel bündig mit dem vorderen 19"-Rahmen abschließen.

- 4) Befestigen Sie das Kommunikationssystem anhand der beiden Haltewinkel [B] mit den dafür vorgesehenen Schrauben am 19"-Schränk.



6.1.3 Wie Sie das Kommunikationssystem an einer Wand befestigen

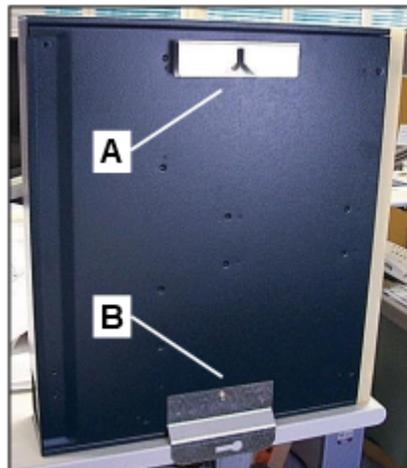
Voraussetzungen

Die Voraussetzungen für die Auswahl des Montagestandorts wurden berücksichtigt (siehe [Voraussetzungen für die Installation](#) auf Seite 31).

Eine tragfähige Wand für die Montage des Kommunikationssystems steht zur Verfügung.

Schritt für Schritt

- 1) Montieren Sie die beiden Haltewinkel [A] und [B] anhand der beiliegenden Schrauben am Gehäuseboden des Kommunikationssystems.



- 2) Bohren Sie ein Loch für den oberen Haltewinkel [A].

- 3) Schieben Sie einen Dübel in das Bohrloch und drehen Sie eine Schraube mit ca. 2 mm Überstand ein.
- 4) Hängen Sie das Kommunikationssystem mit dem oberen Haltewinkel [A] ein.
- 5) Bohren Sie ein Loch für den unteren Haltewinkel [B].
- 6) Schieben Sie einen Dübel in das Bohrloch und befestigen Sie den unteren Haltewinkel [B] mit einer Schraube.

6.2 Schutzerdung

Mit der Schutzerdung wird eine sichere Verbindung zum Erdpotential hergestellt, um bei Auftreten eines Fehlers vor gefährlich hohen Berührungsspannungen zu schützen.



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

- Schutzerden Sie die Kommunikationssysteme OpenScape Business X3R und OpenScape Business X5R durch einen separaten Schutzleiter. Verbinden Sie Ihr Kommunikationssystem vor Inbetriebnahme und Anschluss der Telefone und Leitungen ordnungsgemäß mit dem Schutzleiter.
- Achten Sie auf eine geschützte Verlegung und Zugentlastung des Schutzleiters.

6.2.1 Schutzerdung bei 19"-Schranksmontage

Die Schutzerdung des Kommunikationssystems erfolgt über die Potentialausgleichsschiene des 19"-Schranks.

6.2.1.1 So stellen Sie eine Schutzerdung für das Kommunikationssystem her

Voraussetzungen

Ein Schutzleiter mit einem Mindestquerschnitt von 12 AWG/2,5 mm² und eine Ringklemme sind vorhanden (siehe Abbildung unten). Ein Leiterquerschnitt von mindestens 10 AWG/4 mm² ist erforderlich, um die Auswirkungen externer Faktoren zu blockieren, wenn der Schutzleiter nicht geschützt werden kann.



Ein niederohmiger Masseanschluss ist vorhanden.

Das 19-Zoll-Rack wird mit einem separaten Schutzleiter (grün/gelb) geerdet. Das 19-Zoll-Rack ist mit einer Potenzialausgleichsleiste ausgestattet, an der das Kommunikationssystem separat geerdet werden kann.



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.



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

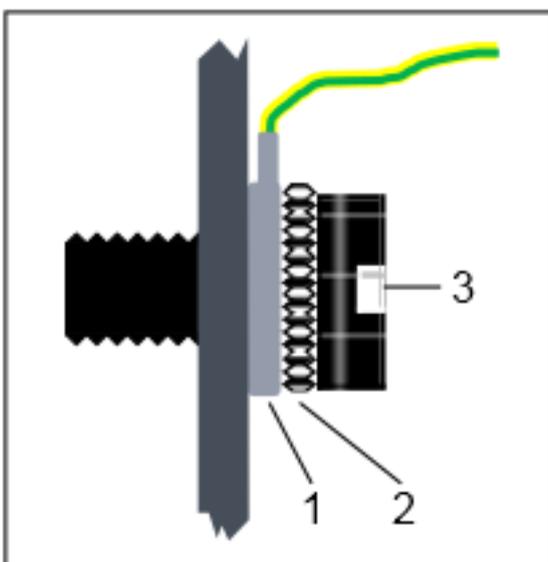
- Schutzerden Sie die Kommunikationssysteme OpenScape Business X3R und in OpenScape Business X5R durch einen separaten Schutzleiter. Verbinden Sie Ihr Kommunikationssystem vor Inbetriebnahme und Anschluss der Telefone und Leitungen ordnungsgemäß mit dem Schutzleiter.
- Achten Sie darauf, dass der Schutzleiter geschützt und zugentlastet ist.

Die in IEC 60364, IEC 60950-1 und IEC 62368-1 angegebenen Ausführungsbestimmungen müssen bei der Installation eingehalten werden.

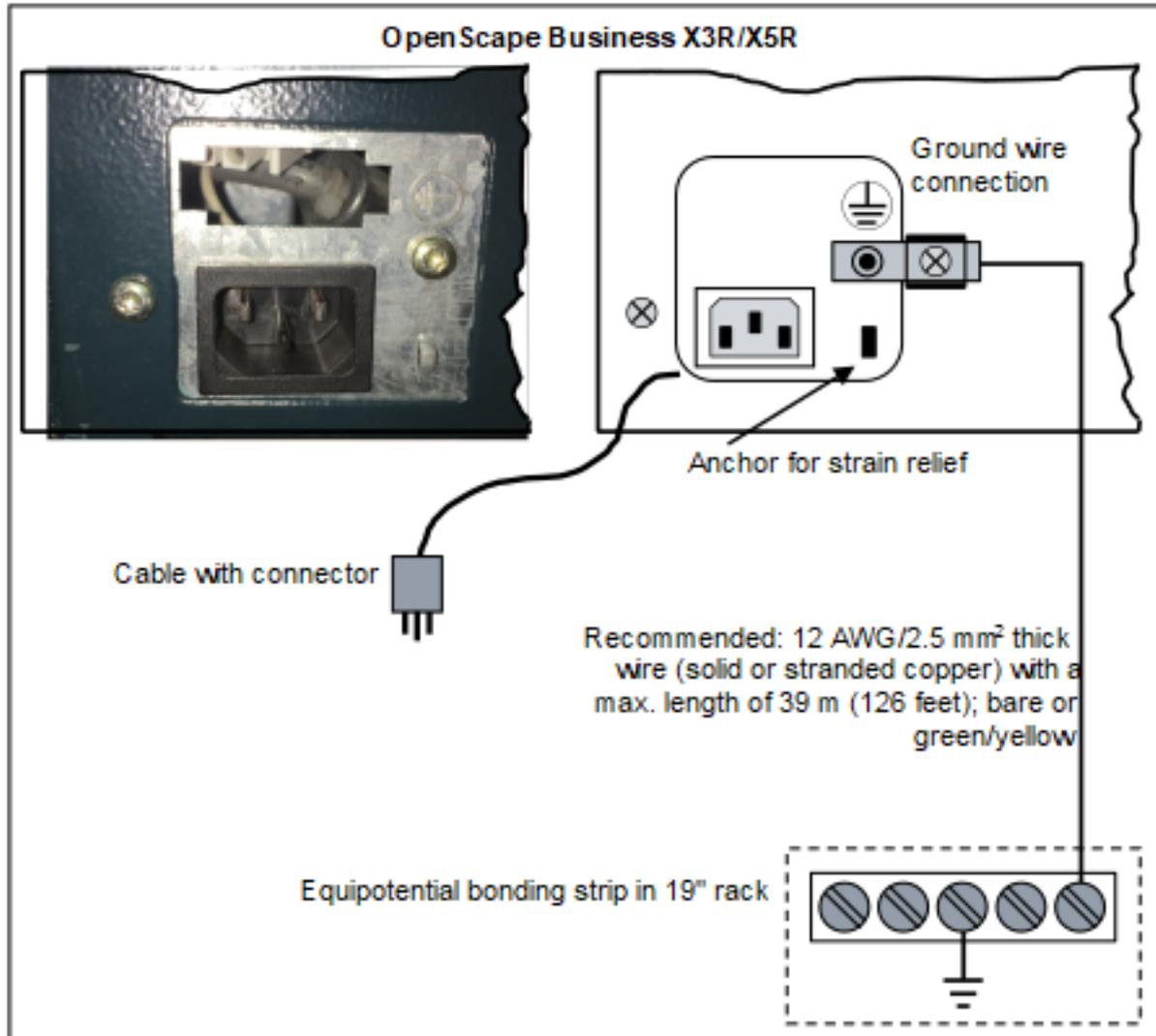
Gehen Sie wie folgt vor, um die Schutzerdung sicherzustellen:

Schritt für Schritt

- 1) Bringen Sie die Ringklemme [1] des separaten Schutzleiters wie in der Abbildung gezeigt mit einer Zahnsicherungsscheibe [2] und einer M4-Schraube [3] am Schutzleiter des Kommunikationssystems an.



- 2) Befestigen Sie den Schutzleiter mit einem Kabelbinder an der entsprechenden Befestigungsöse zur Zugentlastung.
- 3) Verbinden Sie den Schutzleiter mit der Potenzialausgleichsleiste im 19-Zoll-Rack, wie im Schaltdiagramm in der folgenden Abbildung dargestellt.



Achten Sie darauf, dass der Schutzleiter geschützt und zugentlastet ist (Mindestleiterquerschnitt = 12 AWG/2,5 mm²). Ein Leiterquerschnitt von mindestens 10 AWG/4 mm² ist erforderlich, um die Auswirkungen externer Faktoren zu blockieren, wenn der Schutzleiter nicht geschützt werden kann.

6.2.1.2 Wie Sie die Schutzerdung prüfen

Voraussetzungen

Das Kommunikationssystem und alle weiteren Geräte im 19"-Schrank sind nicht über Netzanschlusskabel mit dem Niederspannungsnetz verbunden.

Die separate Schutzerdung für das Kommunikationssystem ist angeschlossen.

Der 19"-Schrank ist durch einen separaten Schutzleiter (grün/gelb) schutzgeerdet.

Führen Sie vor der Inbetriebnahme den folgenden Test durch, um die ordnungsgemäße Schutzerdung des Kommunikationssystems sicherzustellen.

Schritt für Schritt

Prüfen Sie den Ohmschen Widerstand der Schutzleiterverbindung zum Kommunikationssystem:

- a) Die erste Messung erfolgt zwischen dem Schutzkontakt einer Schuko-Steckdose der Hausinstallation und der Potentialausgleichsschiene im 19"-Schrank.
- b) Die zweite Messung erfolgt zwischen der Potentialausgleichsschiene im 19"-Schrank und dem Gehäuse des Kommunikationssystems.

Das Ergebnis (Sollwert) einer Messung muss wesentlich kleiner als 10 Ohm betragen.

Sollten Sie bei einer Messung zu einem anderen Ergebnis kommen, beauftragen Sie einen qualifizierten Elektrotechniker. Dieser muss den Potentialausgleich der Hausinstallation prüfen und die Niederohmigkeit der Schutzleiterverbindung sicherstellen.

6.2.2 Schutzerdung bei Wandmontage und bei freier Aufstellung

Die Schutzerdung des Kommunikationssystems erfolgt zum Beispiel über die Potentialausgleichsschiene des Gebäudes, über eine zusätzliche Anschlussdose an das Niederspannungsnetz, über eine Haupt-Erdsammelschiene oder über ein Erdungsfeld.

6.2.2.1 So stellen Sie eine Schutzerdung für das Kommunikationssystem her

Voraussetzungen

Ein Schutzleiter mit einem Mindestquerschnitt von 12 AWG/2,5 mm² und eine Ringklemme sind vorhanden (siehe Abbildung unten). Ein Leiterquerschnitt von mindestens 10 AWG/4 mm² ist erforderlich, um die Auswirkungen externer Faktoren zu blockieren, wenn der Schutzleiter nicht geschützt werden kann. Bei Verwendung einer zusätzlichen Anschlussdose des Niederspannungsnetzes kann der minimale Leiterquerschnitt auch 16 AWG/1,5 mm² betragen.



Ein niederohmiger Masseanschluss ist vorhanden.



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.



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

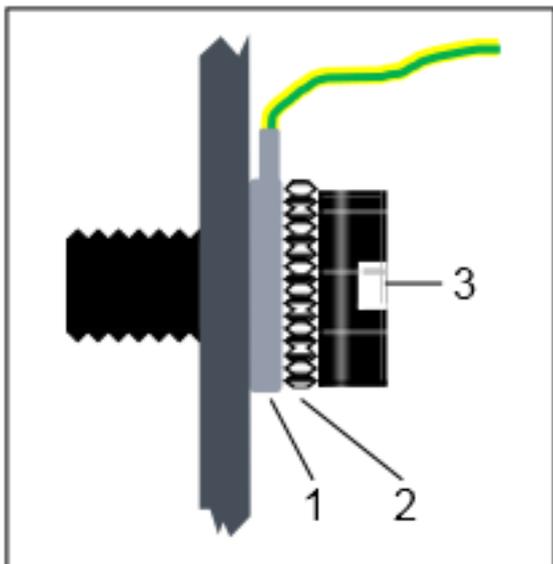
- Schutzerden Sie die Kommunikationssysteme OpenScape Business X3R und in OpenScape Business X5R durch einen separaten Schutzleiter. Verbinden Sie Ihr Kommunikationssystem vor Inbetriebnahme und Anschluss der Telefone und Leitungen ordnungsgemäß mit dem Schutzleiter.
- Achten Sie darauf, dass der Schutzleiter geschützt und zugentlastet ist.

Die in IEC 60364, IEC 60950-1 und IEC 62368-1 angegebenen Ausführungsbestimmungen müssen bei der Installation eingehalten werden.

Gehen Sie wie folgt vor, um die Schutzerdung sicherzustellen:

Schritt für Schritt

- 1) Bringen Sie die Ringklemme [1] des separaten Schutzleiters wie in der Abbildung gezeigt mit einer Zahnsicherungsscheibe [2] und einer M4-Schraube [3] am Schutzleiter des Kommunikationssystems an.



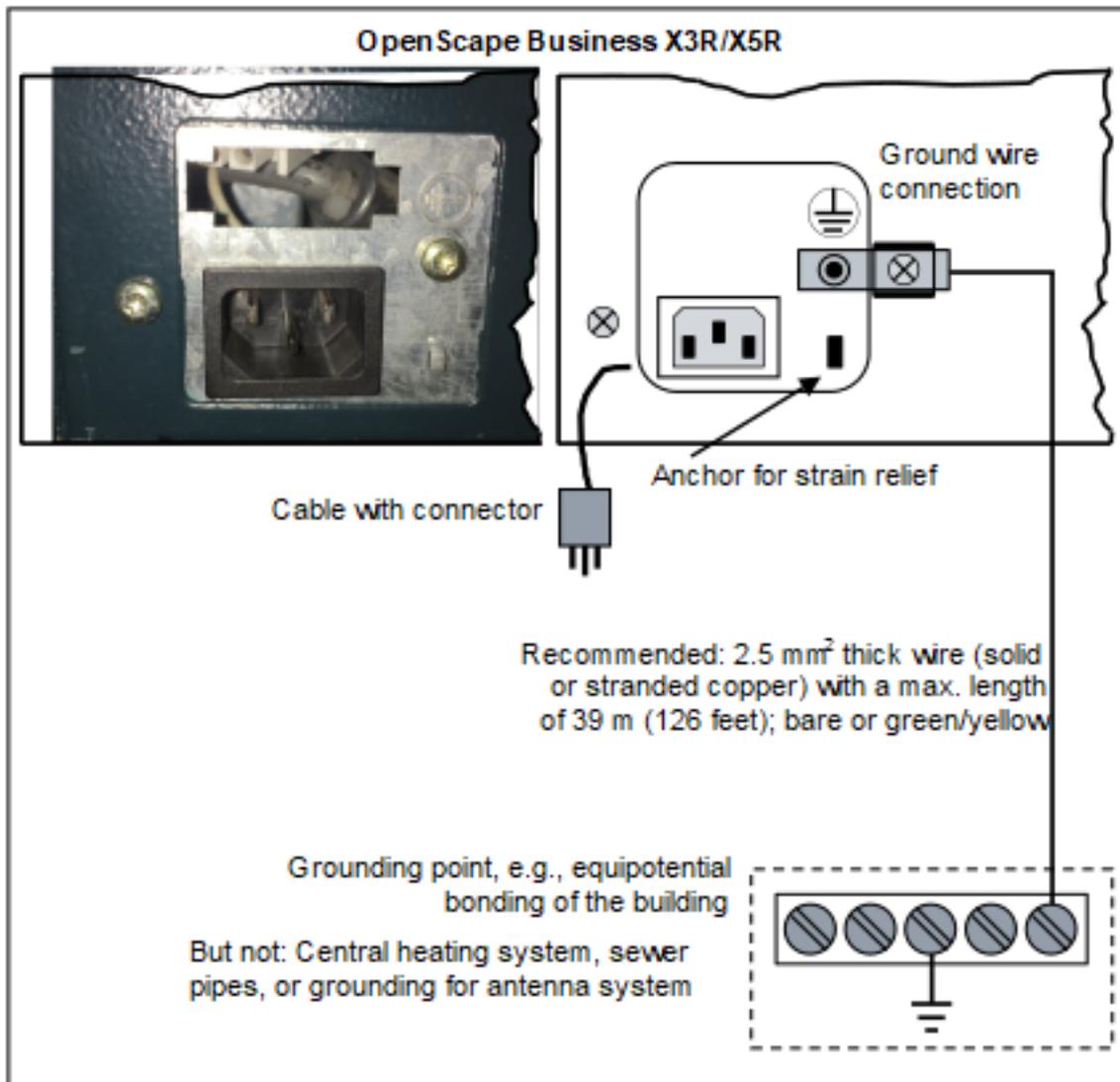
- 2) Befestigen Sie den Schutzleiter mit einem Kabelbinder an der entsprechenden Befestigungsöse zur Zugentlastung.

Hardwareinstallation von OpenScape Business X3R/X5R

3) Wählen Sie eine der folgenden Optionen:

- **Nicht für USA und Kanada - Potenzialausgleichsleiste**

Verbinden Sie den Schutzleiter mit dem Erdungspunkt (z. B. die Potenzialausgleichsleiste des Gebäudes), wie im Schaltdiagramm in der folgenden Abbildung dargestellt.

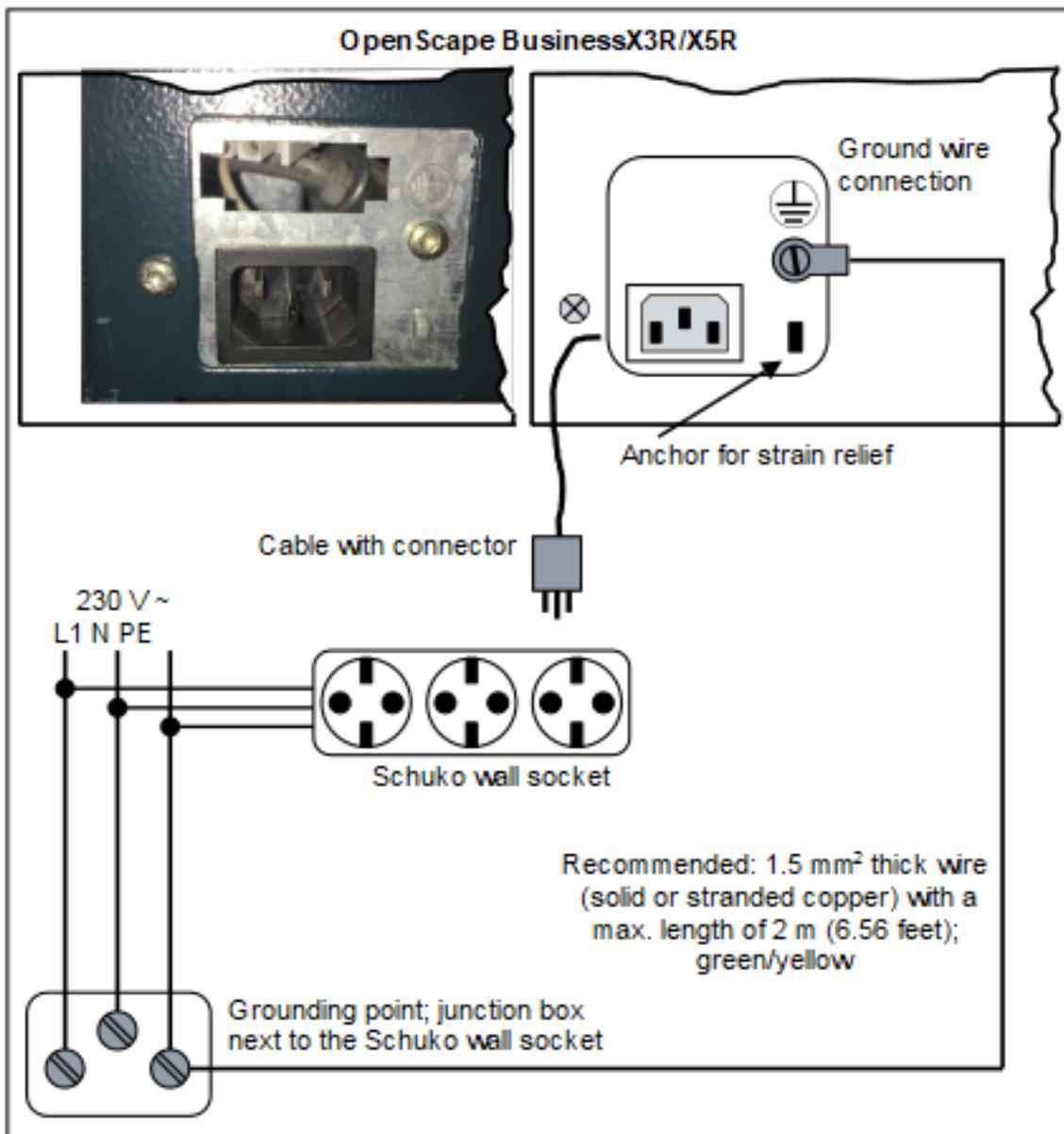


Achten Sie darauf, dass der Schutzleiter geschützt und zugentlastet ist. Der minimale Leiterquerschnitt beträgt 12 AWG/2,5 mm²). Ein Leiterquerschnitt von mindestens 10 AWG/4 mm² ist erforderlich, um die Auswirkungen externer Faktoren zu blockieren, wenn der Schutzleiter nicht geschützt werden kann.

- **Nicht für USA und Kanada - Anschluss an das Niederspannungsnetz**

Schließen Sie eine Anschlussdose in der Nähe der Schuko-Wandsteckdose, an die das Kommunikationssystem angeschlossen ist, an das Niederspannungsnetz an. Verwenden Sie einen separaten

Schutzleiter zum Einrichten einer festen Verbindung mit der Anschlussdose, wie im Schaltdiagramm dargestellt.



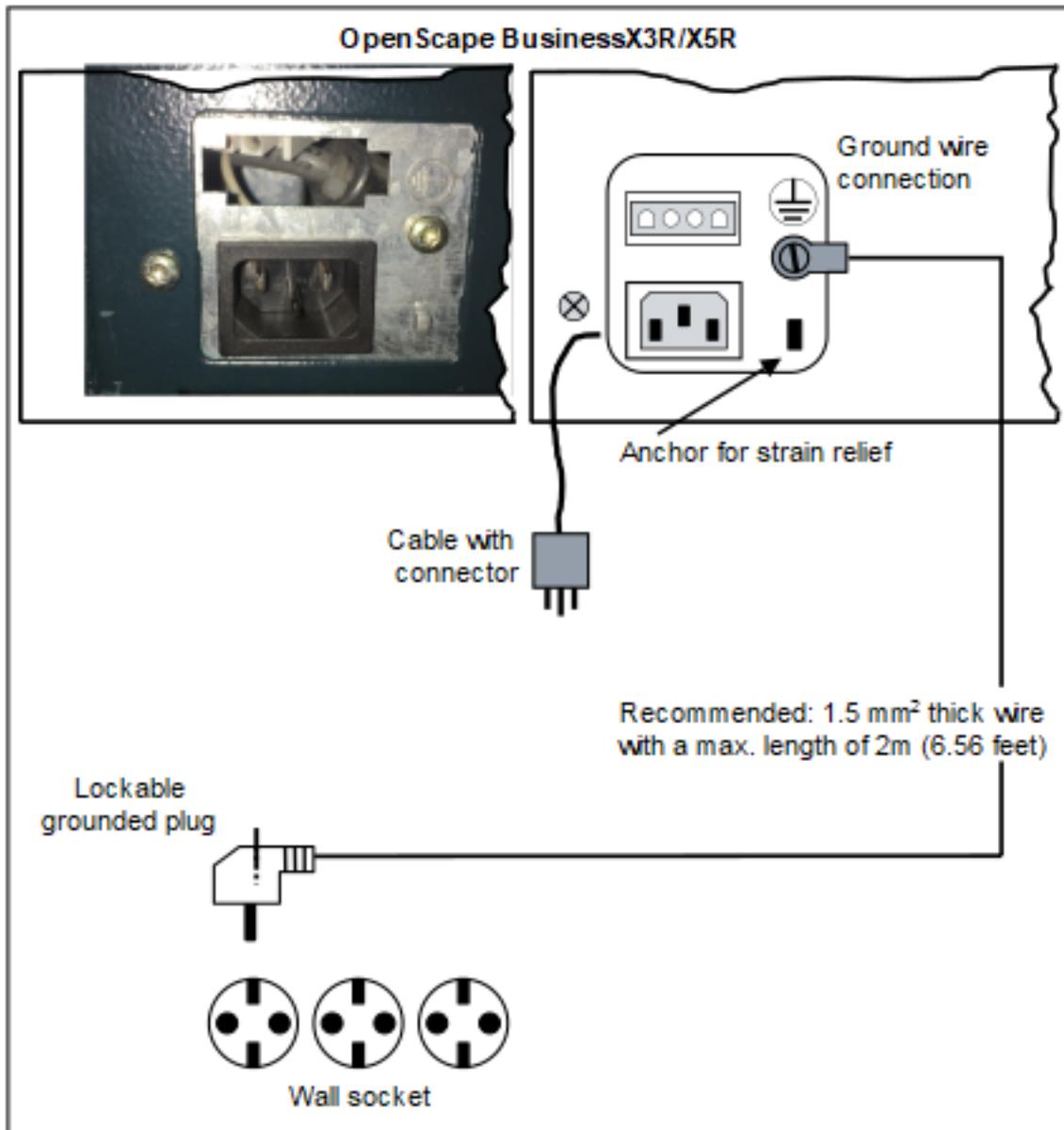
Achten Sie darauf, dass der Schutzleiter geschützt und zugentlastet ist. Der minimale Leiterquerschnitt beträgt 16 AWG/1,5 mm².

- **Nicht für USA und Kanada - Verriegelbarer Schuko-Stecker für Niederspannungsnetz**

Setzen Sie den verriegelbaren Schuko-Stecker (spezieller Schuko mit festem Schutzleiter) in eine Wandsteckdose des Niederspannungsnetzes ein und verriegeln Sie den Stecker. Verwenden Sie den am Stecker angeschlossenen Schutzleiter zum Einrichten einer festen Verbindung mit dem Kommunikationssystem, wie im Schaltdiagramm dargestellt.

Hardwareinstallation von OpenScape Business X3R/X5R

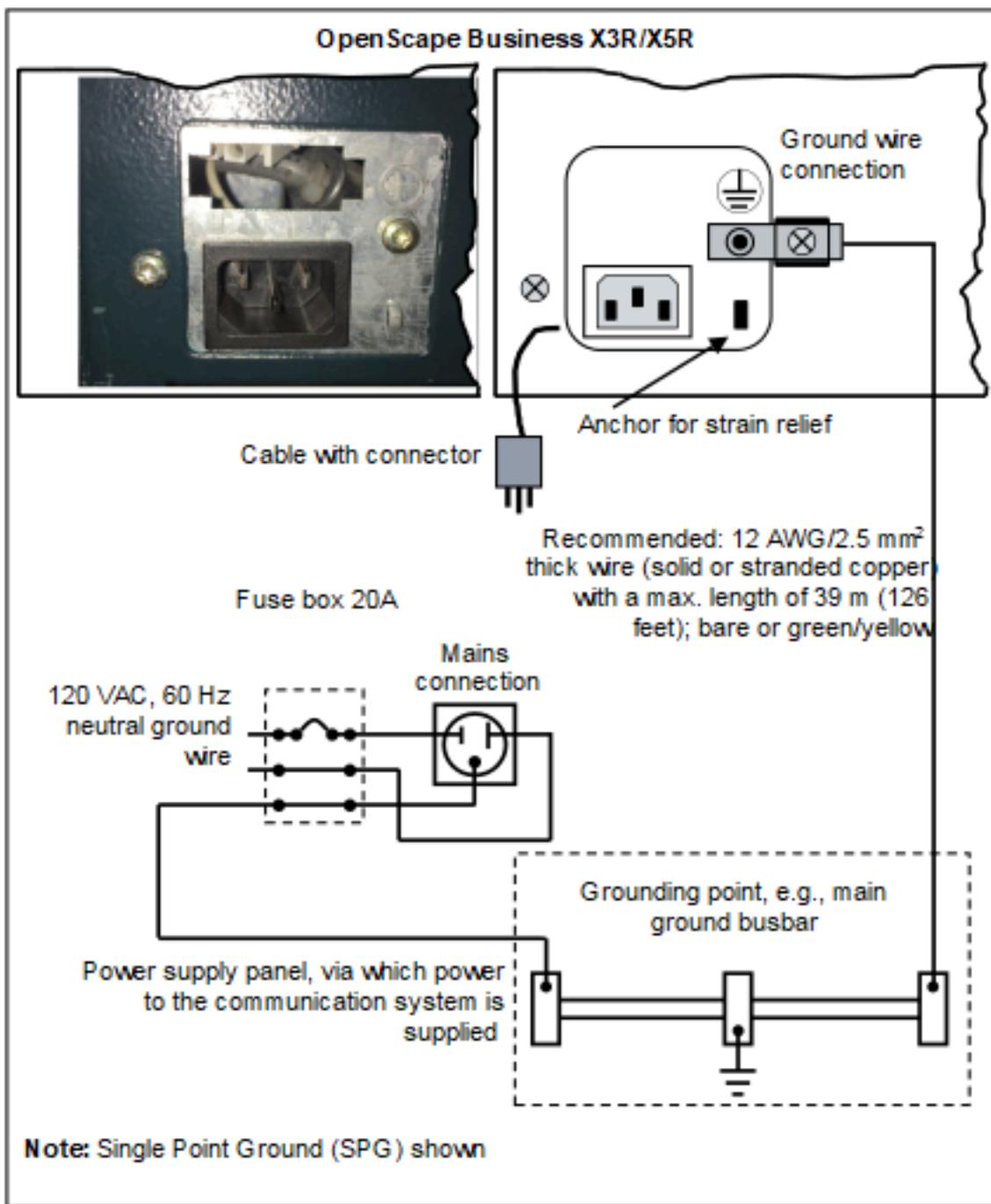
Verwenden Sie einen zweiten verriegelbaren Schuko-Stecker für einen möglicherweise vorhandenen MDFU.



Achten Sie darauf, dass alle verlegten Schutzleiter geschützt und zugentlastet sind. Der minimale Leiterquerschnitt beträgt 16 AWG/1,5 mm² für bis zu 2 m mindestens 12 AWG/2,5 mm² für 2 m und darüber.

- **Nur für USA und Kanada: Haupterdsammelschiene**

Verbinden Sie den Schutzleiter mit dem Erdungspunkt (z. B. Haupterdsammelschiene, Erdungsfeld), wie im Schaltdiagramm in der folgenden Abbildung dargestellt.



Achten Sie darauf, dass alle verlegten Schutzleiter geschützt und zugentlastet sind. Der minimale Leiterquerschnitt beträgt 12 AWG/2,5 mm². Ein Leiterquerschnitt von mindestens 10 AWG/4 mm² ist erforderlich, um die Auswirkungen externer Faktoren zu blockieren, wenn der Schutzleiter nicht geschützt werden kann.

6.2.2.2 Wie Sie die Schutzerdung prüfen

Voraussetzungen

Das Kommunikationssystem ist **noch nicht** über das Netzanschlusskabel mit dem Niederspannungsnetz verbunden.

Die separate Schutzerdung für das Kommunikationssystem ist angeschlossen.

Führen Sie vor der Inbetriebnahme den folgenden Test durch, um die ordnungsgemäße Schutzerdung des Kommunikationssystems sicherzustellen.

Schritt für Schritt

Prüfen Sie den Ohmschen Widerstand der Schutzleiterverbindung zum Kommunikationssystem:

Die Messung erfolgt zwischen dem Schutzkontakt einer Schuko-Steckdose der Hausinstallation (am Anschlussort des Kommunikationssystems) und dem Gehäuse des Kommunikationssystems.

Das Ergebnis (Sollwert) einer Messung muss wesentlich kleiner als 10 Ohm betragen.

Sollten Sie zu einem anderen Messergebnis kommen, beauftragen Sie einen qualifizierten Elektrotechniker. Dieser muss den Potentialausgleich der Hausinstallation prüfen und die Niederohmigkeit der Schutzleiterverbindung sicherstellen.

6.3 Konfigurationshinweise

Die Konfigurationshinweise beinhalten Informationen über die Baugruppen-Steckplätze der Kommunikationssysteme OpenScape Business X3R und OpenScape Business X5R.

6.3.1 Baugruppen-Steckplätze in OpenScape Business X3R

OpenScape Business X3R beinhaltet drei Steckplatzebenen für die Bestückung mit Baugruppen und Optionen.

- Steckplatzebene 1: Steckplätze für zwei Peripheriebaugruppen
- Steckplatzebene 2: Steckplatz für das Mainboard OCCMR
- Steckplatzebene 3: Steckplätze für drei Optionen

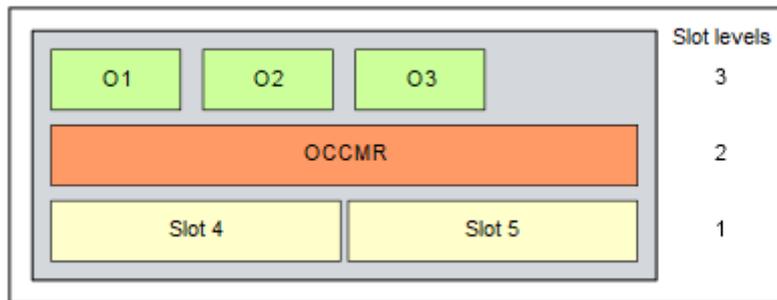


Abbildung 11: OpenScape Business X3R – Baugruppen-Steckplätze

6.3.2 Baugruppen-Steckplätze in OpenScape Business X5R

OpenScape Business X5R beinhaltet fünf Steckplatzebenen für die Bestückung mit Baugruppen und Optionen.

- Steckplatzebenen 1 bis 3: Steckplätze für jeweils zwei Peripheriebaugruppen
- Steckplatzebene 4: Steckplatz für das Mainboard OCCMR
- Steckplatzebene 5: Steckplätze für drei Optionen

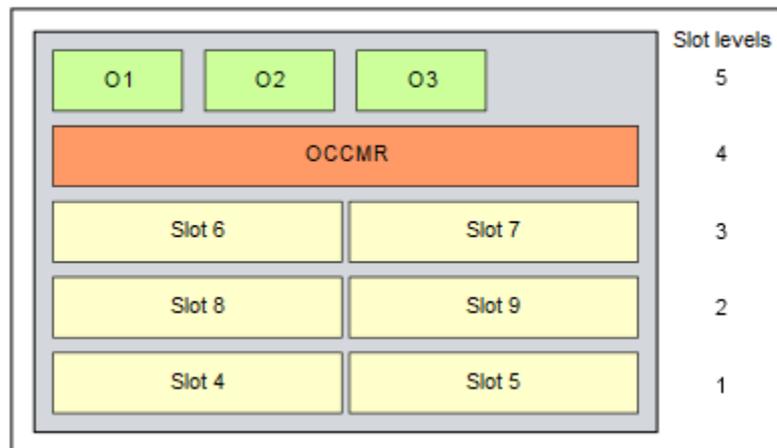


Abbildung 12: OpenScape Business X5R – Baugruppen-Steckplätze

6.3.3 Baugruppeninstallation

6.3.3.1 Wie Sie eine Baugruppe stecken

Voraussetzungen

Ein freier Baugruppen-Steckplatz steht zur Verfügung.

Anmerkung: Grundsätzlich muss beim Arbeiten mit Baugruppen das Erdungsarmband getragen werden.

Die EGB-Schutzmaßnahmen sind zu beachten und zu befolgen (siehe [Warnhinweise: Hinweis](#) auf Seite 16)

Schritt für Schritt

- 1) Lösen Sie die beiden Feststellschrauben in der Abschirmblende des gewünschten Baugruppen-Steckplatzes.
- 2) Ziehen Sie die Abschirmblende ab.
- 3) Schieben Sie die Baugruppe mit Hilfe der Führungsschienen bis zu Anschlag in den Baugruppen-Steckplatz.
- 4) Befestigen Sie die Baugruppe mit den beiden Feststellschrauben am Gehäuse.

6.3.3.2 Wie Sie eine Baugruppe ziehen

Voraussetzungen

Anmerkung: Grundsätzlich muss beim Arbeiten mit Baugruppen das Erdungsarmband getragen werden.

Die EGB-Schutzmaßnahmen sind zu beachten und zu befolgen (siehe [Warnhinweise: Hinweis](#) auf Seite 16)

Schritt für Schritt

- 1) Lösen Sie die beiden Feststellschrauben in der Frontblende der zu entfernenden Baugruppe.
- 2) Ziehen Sie die Baugruppe aus dem Baugruppen-Steckplatz.

6.3.3.3 Wie Sie eine Abschirmblende montieren

Alle leeren Baugruppen-Steckplätze müssen mit einer Abschirmblende versehen sein, damit eine ausreichende Abschirmung gewährleistet ist.

Schritt für Schritt

- 1) Platzieren Sie die Abschirmblende auf den leeren Baugruppen-Steckplatz.
- 2) Befestigen Sie die Abschirmblende mit den beiden Feststellschrauben am Gehäuse.

6.4 Amtsanschluss

Die Kommunikationssysteme OpenScape Business X3R und OpenScape Business X5R bieten verschiedene Möglichkeiten für den Amtsanschluss und damit für den Zugang zum öffentlichen Kommunikationsnetz.

Wählen Sie den oder die für Ihr Kommunikationssystem erforderlichen Amtsanschlüsse unter folgenden Möglichkeiten aus:

- ISDN-Anlagenanschluss und ISDN-Mehrgeräteanschluss über S₀-Schnittstelle (nicht für USA, Kanada)

- Nur für OpenScape Business X5R: ISDN-Primärmultiplexanschluss über S_{2M}-Schnittstelle (nicht für USA, Kanada)
- Nur für OpenScape Business X5R: ISDN-Primärmultiplexanschluss über T1-Schnittstelle (nur für USA, Kanada)
- Nur für OpenScape Business X5R: Amtsanschluss mit CAS-Protokoll über CAS-Schnittstelle (nur für ausgewählte Länder)
- Analoges Amtsanschluss

6.4.1 Nicht für USA, Kanada: Wie Sie einen ISDN-Anlagen- oder ISDN-Mehrgeräteanschluss über die S₀-Schnittstelle durchführen

Voraussetzungen



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen
Schutzerden Sie Ihr Kommunikationssystem vor Anschluss der Telefone und Leitungen durch separate Schutzleiter.



ACHTUNG:

Brandgefahr

Um das Brandrisiko zu verringern, dürfen Sie nur Kommunikationsleitungen mit einem Leiterdurchmesser von mindestens 0,4 mm (AWG 26) oder größer verwenden.

Mindestens eine freie S₀-Schnittstelle steht zur Verfügung (Mainboard OCCMR oder Peripheriebaugruppe STLSX4R, STLS4R).

Die verwendete S₀-Schnittstelle muss bei der Inbetriebnahme als ISDN-Anlagen- oder ISDN-Mehrgeräteanschluss konfiguriert werden.

Ein ISDN-Anlagen- oder ISDN-Mehrgeräteanschluss steht zur Verfügung.

Schritt für Schritt

Verbinden Sie den gewünschten S₀-Anschluss mit dem NTBA des ISDN-Anlagen- oder ISDN-Mehrgeräteanschlusses.

6.4.2 Nicht für USA, Kanada: Wie Sie einen ISDN-Primärmultiplexanschluss über die S_{2M}-Schnittstelle durchführen (nur für OpenScape Business X5R)

Voraussetzungen



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

Schutzerden Sie Ihr Kommunikationssystem vor Anschluss der Telefone und Leitungen durch separate Schutzleiter.



ACHTUNG:

Brandgefahr

Um das Brandrisiko zu verringern, dürfen Sie nur Kommunikationsleitungen mit einem Leiterdurchmesser von mindestens 0,4 mm (AWG 26) oder größer verwenden.

OpenScape Business X5R ist mit einer Baugruppe TS2RN bestückt.

Ein ISDN-Primärmultiplexanschluss steht zur Verfügung.

Schritt für Schritt

Verbinden Sie die S_{2M}-Schnittstelle mit dem NTPM des ISDN-Primärmultiplexanschlusses.

6.4.3 Nur für USA, Kanada: Wie Sie einen ISDN-Primärmultiplexanschluss über die T1-Schnittstelle durchführen (nur für OpenScape Business X5R)

Voraussetzungen



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

Schutzerden Sie Ihr Kommunikationssystem vor Anschluss der Telefone und Leitungen durch separate Schutzleiter.



ACHTUNG:

Brandgefahr

Um das Brandrisiko zu verringern, dürfen Sie nur Kommunikationsleitungen mit einem Leiterdurchmesser von mindestens 0,4 mm (AWG 26) oder größer verwenden.

OpenScape Business X5R ist mit einer Baugruppe TST1R bestückt.

Eine Channel Service Unit (CSU) steht zur Verfügung, die nach FCC Part 68 zugelassen ist und die ANSI-Vorschrift T1.403 erfüllt. Die T1-Schnittstelle darf nicht direkt mit dem PSTN (Public Switched Telephone Network) verbunden werden. Es ist erforderlich, eine CSU zwischen Kommunikationssystem und digitalem Amtsanschluss zu schalten. Durch die CSU erhält OpenScape Business X5R folgende Merkmale: Isolierung und Überspannungsschutz des Kommunikationssystems, Diagnosemöglichkeiten im Fehlerfall (zum Beispiel Signal Loop Back, Einfügen von Testsignalen und Testmustern), Einpegeln des Ausgangssignals entsprechend den vom Netzanbieter vorgeschriebenen Leitungslängen. Eine CSU ist kein Lieferbestandteil des Kommunikationssystems OpenScape Business X5R.

Ein ISDN-Primärmultiplexanschluss steht zur Verfügung.

Schritt für Schritt

Verbinden Sie die T1-Schnittstelle mit der Channel Service Unit (CSU).

6.4.4 Nur für ausgewählte Länder: Wie Sie einen Amtsanschluss über die E1-CAS-Schnittstelle durchführen (nur für OpenScape Business X5R)

Voraussetzungen



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

Schutzerden Sie Ihr Kommunikationssystem vor Anschluss der Telefone und Leitungen durch separate Schutzleiter.



ACHTUNG:

Brandgefahr

Um das Brandrisiko zu verringern, dürfen Sie nur Kommunikationsleitungen mit einem Leiterdurchmesser von mindestens 0,4 mm (AWG 26) oder größer verwenden.

OpenScape Business X5R ist mit einer Baugruppe TCASR-2 bestückt.

Ein Amtsanschluss mit CAS-Protokoll steht zur Verfügung.

Schritt für Schritt

Verbinden Sie die gewünschte CAS-Schnittstelle der Baugruppe TCASR-2 mit dem NT des Amtsanschlusses.

6.4.5 Wie Sie einen analogen Amtsanschluss durchführen

Voraussetzungen



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

Schutzerden Sie Ihr Kommunikationssystem vor Anschluss der Telefone und Leitungen durch separate Schutzleiter.



ACHTUNG:

Brandgefahr

Hardwareinstallation von OpenScape Business X3R/X5R

Anschluss von Telefonen und Geräten

Um das Brandrisiko zu verringern, dürfen Sie nur Kommunikationsleitungen mit einem Leiterdurchmesser von mindestens 0,4 mm (AWG 26) oder größer verwenden.

Anmerkung:

Brandgefahr durch Überspannung

Bei Leitungslängen über 500 m und bei Leitungen, die das Gebäude verlassen, muss die Baugruppe TLANI4R durch einen externen Blitzschutz geschützt werden.

Ein solcher Blitzschutz wird als zusätzlicher Primärschutz bezeichnet. Der zusätzliche Primärschutz wird durch den 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.

Das Kommunikationssystem ist mit mindestens einer Baugruppe TLANI4R bestückt.

Nur für USA, Kanada: Ein Sicherungselement gemäß UL 497A oder CSA C22.2 No. 226 steht zur Verfügung. Die Installationsvorschriften erfordern, dass der Anschluss der analogen Amtsleitungen über Sicherungselemente gemäß UL 497A oder CSA C22.2 No. 226 erfolgen muss.

Ein analoger Amtsanschluss mit HKZ (Hauptanschlusskennzeichen)-Signalisierungsverfahren (Ground Start oder Loop Start) steht zur Verfügung.

Schritt für Schritt

Verbinden Sie den gewünschten a/b-Anschluss der gewünschten Baugruppe mit der TAE-Anschlussdose des analogen Amtsanschlusses.

6.5 Anschluss von Telefonen und Geräten

Die Kommunikationssysteme OpenScape Business X3R und OpenScape Business X5R bieten verschiedene Optionen für den Anschluss von Telefonen und Geräten.

Sie können den oder die erforderlichen Anschlüsse für Ihr Kommunikationssystem aus den folgenden Optionen wählen:

- Direkter Anschluss von ISDN-Telefonen (nicht für USA und Kanada)
- Anschluss von ISDN-Telefonen über den S₀-Bus (nicht für USA und Kanada)
- Anschluss von U_{P0/E}-Telefonen
- Anschluss von analogen Telefonen und Geräten

Anmerkung: An eine a/b-Schnittstelle kann nur ein analoges Gerät angeschlossen werden.

6.5.1 Nicht für USA, Kanada: Wie Sie ISDN-Telefone direkt anschließen

Voraussetzungen



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

Schutzerden Sie Ihr Kommunikationssystem vor Anschluss der Telefone und Leitungen durch separate Schutzleiter.



ACHTUNG:

Brandgefahr

Um das Brandrisiko zu verringern, dürfen Sie nur Kommunikationsleitungen mit einem Leiterdurchmesser von mindestens 0,4 mm (AWG 26) oder größer verwenden.

Anmerkung:

Brandgefahr durch Überspannung

Nur für die für den Teilnehmeranschluss verwendeten Schnittstellen: Bei Leitungslängen über 500 m und bei Leitungen, die das Gebäude verlassen, müssen die Baugruppen OCCMR, STLSX4R und STLS4R durch einen externen Blitzschutz geschützt werden.

Ein solcher Blitzschutz wird als zusätzlicher Primärschutz bezeichnet. Der zusätzliche Primärschutz wird durch den 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.

Mindestens eine freie S₀-Schnittstelle steht zur Verfügung (Mainboard OCCMR oder Peripheriebaugruppe STLSX4R, STLS4R).

Die verwendeten S₀-Schnittstellen müssen bei der Inbetriebnahme als interner S₀-Anschluss konfiguriert werden.

Die anzuschließenden ISDN-Telefone müssen über eine eigene Speisung verfügen, zum Beispiel über ein Steckernetzgerät. Eine Speisung über die S₀-Schnittstellen der Baugruppen OCCMR, STLSX4R und STLS4R ist nicht möglich.

Schritt für Schritt

- 1) Verbinden Sie den gewünschten S₀-Anschluss mit ISDN-Telefon.

Tipp:

Beachten Sie die Angaben in der Installationsanleitung des anzuschließenden Telefons.

- 2) Falls gewünscht, verbinden Sie weitere ISDN-Telefone auf die gleiche Weise mit dem Kommunikationssystem.

6.5.2 Nicht für USA, Kanada: Wie Sie ISDN-Telefone über den S₀-Bus anschließen

Voraussetzungen



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

Schutzerden Sie Ihr Kommunikationssystem vor Anschluss der Telefone und Leitungen durch separate Schutzleiter.



ACHTUNG:

Brandgefahr

Um das Brandrisiko zu verringern, dürfen Sie nur Kommunikationsleitungen mit einem Leiterdurchmesser von mindestens 0,4 mm (AWG 26) oder größer verwenden.

Anmerkung:

Brandgefahr durch Überspannung

Nur für die für den Teilnehmeranschluss verwendeten Schnittstellen: Bei Leitungslängen über 500 m und bei Leitungen, die das Gebäude verlassen, müssen die Baugruppen OCCMR, STLSX4R und STLS4R durch einen externen Blitzschutz geschützt werden.

Ein solcher Blitzschutz wird als zusätzlicher Primärschutz bezeichnet. Der zusätzliche Primärschutz wird durch den 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.

Mindestens eine freie S₀-Schnittstelle steht zur Verfügung (Mainboard OCCMR oder Peripheriebaugruppe STLSX4R, STLS4R).

Die verwendeten S₀-Schnittstellen müssen bei der Inbetriebnahme als interner S₀-Anschluss konfiguriert werden.

Die anzuschließenden ISDN-Telefone müssen über eine eigene Speisung verfügen, zum Beispiel über ein Steckernetzgerät. Eine Speisung über die S₀-Schnittstellen der Baugruppen OCCMR, STLSX4R und STLS4R ist nicht möglich.

Jedem einzelnen ISDN-Telefon (ISDN-Teilnehmer) muss eine eindeutige Multiple Subscriber Number MSN zugeordnet werden. Diese Zuordnung ist im Konfigurationsmenü des ISDN-Teilnehmers durchzuführen.

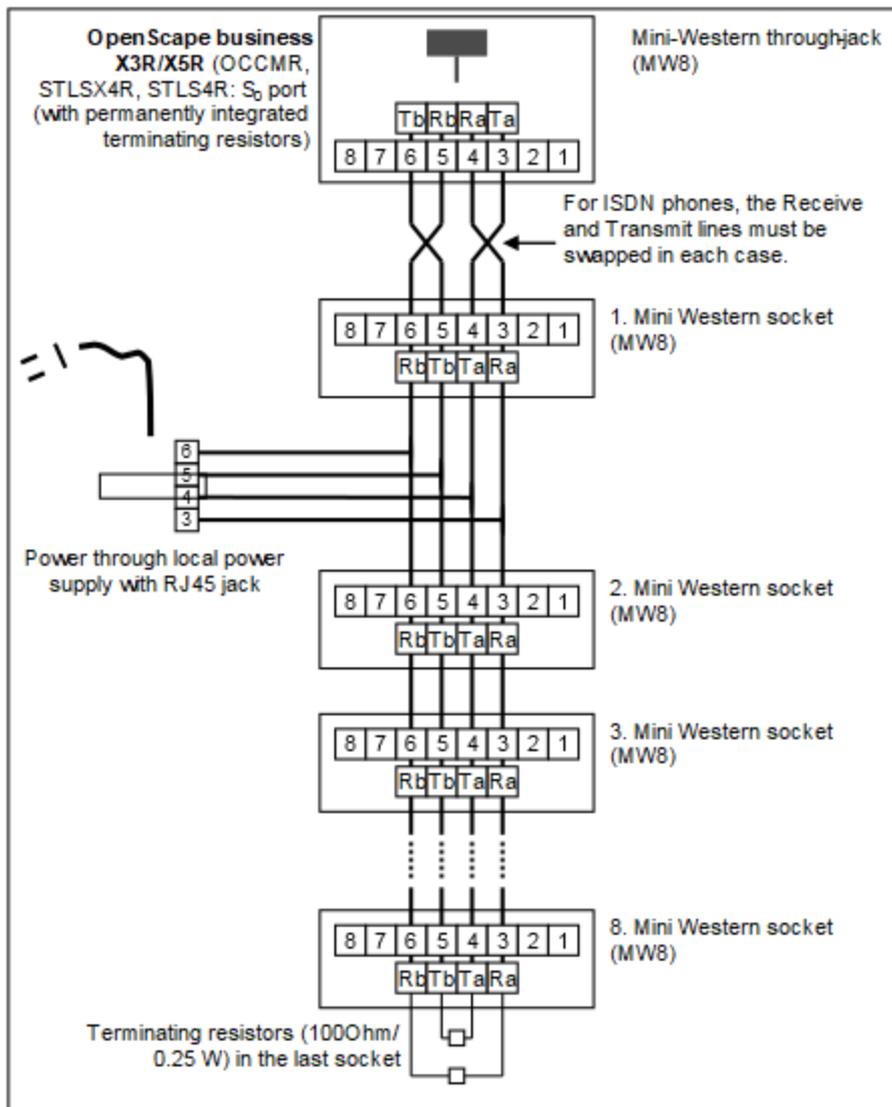
Schritt für Schritt

- 1) Verbinden Sie den gewünschten S₀-Anschluss mit der Mini-Western-Durchgangsdose des S₀-Busses.

Tipp:

Beachten Sie die Angaben in der Installationsanleitung des anzuschließenden Telefons.

2) Führen Sie weitere Verdrahtung wie im folgenden Bild gezeigt durch.



- 3) Montieren Sie Abschlusswiderstände (100 Ohm/0,25 W) in der letzten Anschlussdose des S₀-Busses.
- 4) Stellen Sie sicher, dass nur an den beiden Enden des S₀-Busses Abschlusswiderstände vorhanden sind. Die weiteren Anschlussdosen des S₀-Busses benötigen keine Abschlusswiderstände.

Tipp:

Da Abschlusswiderstände in OpenScape Business X3R und OpenScape Business X5R bereits fest integriert sind, bildet das Kommunikationssystem das eine Ende eines S₀-Busses.

Tipp:

Beachten Sie die Angaben in der Installationsanleitung des anzuschließenden Telefons.

6.5.3 Wie Sie U_{P0/E}-Telefone anschließen

Voraussetzungen



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen
Schutzerden Sie Ihr Kommunikationssystem vor Anschluss der Telefone und Leitungen durch separate Schutzleiter.



ACHTUNG:

Brandgefahr

Um das Brandrisiko zu verringern, dürfen Sie nur Kommunikationsleitungen mit einem Leiterdurchmesser von mindestens 0,4 mm (AWG 26) oder größer verwenden.

Anmerkung:

Brandgefahr durch Überspannung

Bei Leitungslängen über 500 m und bei Leitungen, die das Gebäude verlassen, müssen die Baugruppen OCCMR und SLU8R durch einen externen Blitzschutz geschützt werden.

Ein solcher Blitzschutz wird als zusätzlicher Primärschutz bezeichnet. Der zusätzliche Primärschutz wird durch den 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.

Mindestens eine freie U_{P0/E}-Schnittstelle steht zur Verfügung (Mainboard OCCMR oder Peripheriebaugruppe SLU8R).

Schritt für Schritt

- 1) Verbinden Sie den gewünschten U_{P0/E}-Anschluss mit dem U_{P0/E}-Telefon.
-

Tipp:

Beachten Sie die Angaben in der Installationsanleitung des anzuschließenden Telefons.

- 2) Falls gewünscht, verbinden Sie weitere U_{P0/E}-Telefone auf die gleiche Weise mit dem Kommunikationssystem.

6.5.4 Wie Sie analoge Telefone und Geräte anschließen

Voraussetzungen



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

Schutzerden Sie Ihr Kommunikationssystem vor Anschluss der Telefone und Leitungen durch separate Schutzleiter.



ACHTUNG:

Brandgefahr

Um das Brandrisiko zu verringern, dürfen Sie nur Kommunikationsleitungen mit einem Leiterdurchmesser von mindestens 0,4 mm (AWG 26) oder größer verwenden.

Anmerkung:

Brandgefahr durch Überspannung

Bei Leitungslängen über 500 m und bei Leitungen, die das Gebäude verlassen, müssen die Baugruppen OCCMR, SLAD8R und 8SLAR durch einen externen Blitzschutz geschützt werden.

Ein solcher Blitzschutz wird als zusätzlicher Primärschutz bezeichnet. Der zusätzliche Primärschutz wird durch den 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.

Mindestens eine freie a/b-Schnittstelle steht zur Verfügung (Mainboard OCCMR oder Peripheriebaugruppe SLAD8R, 8SLAR).

Schritt für Schritt

- 1) Verbinden Sie den gewünschten a/b-Anschluss mit dem anzuschließenden analogen Telefon oder analogen Gerät (Fax, Modem, TFE-S usw.).
-

Tipp:

Beachten Sie die Angaben in der Installationsanleitung des anzuschließenden Telefons/Geräts.

- 2) Falls gewünscht, verbinden Sie weitere analoge Telefone oder Geräte auf die gleiche Weise mit dem Kommunikationssystem.

6.6 Abschließende Tätigkeiten

Zum Abschluss der Montage ist die SDHC-Karte zu stecken, eine Sichtkontrolle durchzuführen und das System an das Stromnetz zu nehmen.

Anschließend kann das Kommunikationssystem mit dem OpenScape Business Assistant (WBM) in Betrieb genommen werden. Die Beschreibung dazu finden Sie in der Online-Hilfe des WBM oder in der Administrator Dokumentation im Kapitel "Erstinstallation OpenScape Business".

Anmerkung: Bei der Erstinbetriebnahme des Kommunikationssystems ist der Ladezustand des Akkus auf dem Mainboard nicht definiert. Um einen ausreichenden Ladezustand zu erreichen, muss das System mindestens 2 Tage am Stromnetz bleiben. Wird das System vom Stromnetz getrennt, kann es bei unzureichendem Ladezustand des Akkus vorkommen, dass die Activation Period wegen Zeitmanipulation gesperrt wird.

6.6.1 So setzen Sie die M.2 SSD oder die SDHC-Karte ein (System mit OCCM)

Die M.2 SSD oder die SDHC-Karte enthält die OpenScape Business Kommunikationssoftware und muss vor dem Starten des Kommunikationssystems eingebaut/eingesetzt werden.

Schritt für Schritt

- 1) Vergewissern Sie sich, dass der Schreibschutz der SDHC-Karte deaktiviert ist (Schalter Richtung Metallkontakte).
- 2) Stecken Sie die SDHC-Karte in den SDHC-Steckplatz des Mainboards, bis sie einrastet. Die Metallkontakte der SDHC-Karte müssen dabei Richtung Mainboard zeigen.

6.6.2 Wie Sie eine Sichtkontrolle durchführen

Vor Inbetriebnahme des Kommunikationssystems muss eine Sichtkontrolle der Hardware, der Verkabelung und der Spannungsversorgung durchgeführt werden.

Voraussetzungen



GEFAHR:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

Trennen Sie sämtliche Versorgungsstromkreise des Kommunikationssystems, bevor Sie mit der Sichtkontrolle beginnen:

- Schalten Sie Akkuspannung, Speisespannung (LUNA2) und Netzspannung einer eventuell angeschlossenen OpenScape Business Powerbox ab.

- Ziehen Sie die Anschlussleitungen einer eventuell angeschlossenen OpenScape Business Powerbox.
- Ziehen Sie die Anschlussleitungen eines eventuell angeschlossenen Akkupacks oder eventuell angeschlossener Akkus.
- Ziehen Sie den Netzanschlussstecker des Kommunikationssystems.

Anmerkung:

Grundsätzlich muss beim Arbeiten mit Baugruppen das Erdungsarmband getragen werden.

Die EGB-Schutzmaßnahmen sind zu beachten und zu befolgen (siehe [Warnhinweise: Hinweis](#) auf Seite 16).

Schritt für Schritt

- 1) Trennen Sie sämtliche Versorgungsstromkreise des Kommunikationssystems.
- 2) Prüfen Sie, ob das Kommunikationssystem spannungsfrei ist.
- 3) Prüfen Sie, ob die SDHC-Karte korrekt eingerastet ist. Der Schreibschutz der SDHC-Karte muss deaktiviert sein (Schalter Richtung Metallkontakte).
- 4) Prüfen Sie sämtliche Baugruppen auf festen Sitz.
Falls erforderlich, sorgen Sie für das korrekte Stecken der betroffenen Baugruppen (siehe [Wie Sie eine Baugruppe stecken](#)).
- 5) Prüfen Sie das Vorhandensein von Abschirmblenden bei leeren Baugruppen-Steckplätzen.
Falls erforderlich, montieren Sie die fehlenden Abschirmblenden (siehe [Wie Sie eine Abschirmblende montieren](#)).
- 6) Prüfen Sie die korrekte Verlegung aller Anschluss- und Verbindungskabel. Sind beispielsweise Stolpergefahren vorhanden?
Falls erforderlich, sorgen Sie für eine korrekte Verlegung der Anschluss- und Verbindungskabel.
- 7) Prüfen Sie, ob ein separat geführter Schutzleiter am Schutzleiteranschluss des Kommunikationssystems angeschlossen ist.
Falls erforderlich, führen Sie die separate Schutzerdung des Kommunikationssystems durch (siehe [Schutzerdung bei 19"-Schrankmontage](#) und [Schutzerdung bei Wandmontage und bei freier Aufstellung](#)).
- 8) Prüfen Sie, ob die Nennspannung der Netzspannungsversorgung mit der Nennspannung des Kommunikationssystems (Typenschild) übereinstimmt.

6.6.3 Wie Sie das System ans Stromnetz anschließen

Schritt für Schritt

Stecken Sie das Netzanschlusskabel in die Buchse der Stromversorgung. Das Kommunikationssystem fährt hoch.

Anmerkung: Lassen Sie das System mindestens 2 Tage am Stromnetz, damit der Akku des Mainboards einen

ausreichenden Ladezustand erreicht. Bei unzureichendem Ladezustand kann es vorkommen, dass bei wiederholtem Hochfahren des Systems die Activation Period wegen Zeitmanipulation gesperrt wird.

7 Hardwareinstallation von OpenScape Business X8

Beschrieben ist die vorwiegend durchgeführte Standardmontage des Kommunikationssystems OpenScape Business X8.

OpenScape Business X8 ist ein modulares Kommunikationssystem, das als Einboxsystem (Basisbox) oder als Zweiboxsystem (Basisbox + Erweiterungsbox) eingesetzt werden kann. OpenScape Business X8 kann frei aufgestellt oder in einen 19"-Schrank montiert werden.



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

- Arbeiten am geöffneten Gehäuse dürfen nur im spannungsfreien Zustand durchgeführt werden.
- Prüfen Sie vor Beginn jeder Arbeit, ob alle Stromkreise spannungsfrei sind. Halten Sie es nie für selbstverständlich, dass mit Ausschalten einer Sicherung oder eines Hauptschalters alle Stromkreise auch zuverlässig unterbrochen sind.

7.1 Montagearten

OpenScape Business X8 kann frei aufgestellt oder in einen 19"-Schrank montiert werden.

7.1.1 Freistehende Montage

OpenScape Business X8 ist ein modulares Kommunikationssystem, das als Einboxsystem (Basisbox) oder als Zweiboxsystem (Basisbox + Erweiterungsbox) eingesetzt werden kann. Bei einem Zweiboxsystem können die Systemboxen aufeinander oder nebeneinander aufgestellt werden.

7.1.1.1 Wie Sie ein Einboxsystem aufstellen

Voraussetzungen

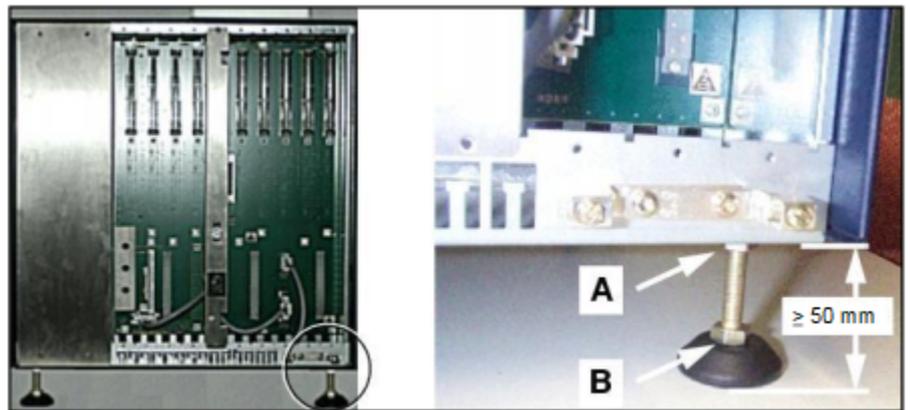
Die Voraussetzungen für die Auswahl des Montagestandorts bei freistehender Montage wurden berücksichtigt (siehe [Voraussetzungen für die Installation](#) auf Seite 31).

Die vordere und hintere Kunststoffabdeckung der Systembox ist nicht montiert.

Schritt für Schritt

- 1) Platzieren Sie die Systembox am Montageort und sorgen Sie für einen festen und ebenen Stand.
- 2) Prüfen Sie, ob der Mindestabstand von 50 mm zwischen Unterkante der Systembox und Boden nicht unterschritten wird.

- 3) Falls erforderlich, richten Sie die Systembox folgendermaßen aus:
- Lösen Sie die Kontermutter [A] eines Standfußes mit Hilfe eines Gabelschlüssels (Schlüsselweite = 13 mm).
 - Ändern Sie die Höhe des Standfußes durch Drehen der Schraubmutter [B] so, dass die Systembox gerade steht und der Mindestabstand eingehalten wird.
 - Fixieren Sie den Standfuß durch Festdrehen der Kontermutter [A].
 - Falls erforderlich, wiederholen Sie die Schritte a bis c für weitere Standfüße, bis die Systembox gerade steht und der Mindestabstand eingehalten wird.



7.1.1.2 Zweiboxsystem: Wie Sie die Systemboxen aufeinander aufstellen

Voraussetzungen

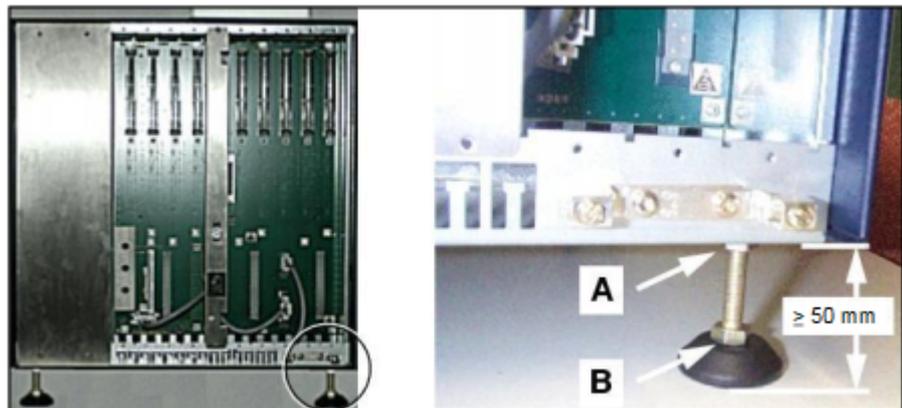
Die Voraussetzungen für die Auswahl des Montagestandorts bei freistehender Montage wurden berücksichtigt (siehe [Voraussetzungen für die Installation](#) auf Seite 31).

Die vordere und hintere Kunststoffabdeckung der Systemboxen ist nicht montiert.

Schritt für Schritt

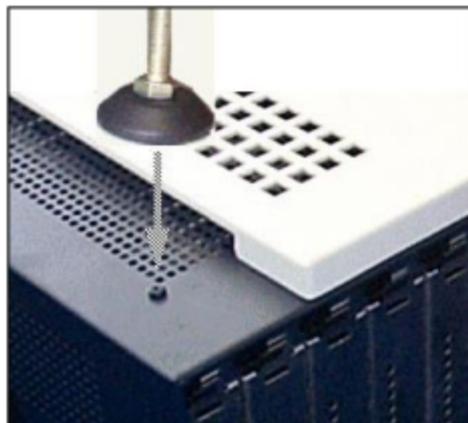
- Platzieren Sie die Basisbox am Montageort und sorgen Sie für einen festen und ebenen Stand.
- Prüfen Sie, ob der Mindestabstand von 50 mm zwischen Unterkante der Basisbox und Boden nicht unterschritten wird.

- 3) Falls erforderlich, richten Sie die Basisbox folgendermaßen aus:
 - a) Lösen Sie die Kontermutter [A] eines Standfußes mit Hilfe eines Gabelschlüssels (Schlüsselweite = 13 mm).
 - b) Ändern Sie die Höhe des Standfußes durch Drehen der Schraubmutter [B] so, dass die Basisbox gerade steht und der Mindestabstand eingehalten wird.
 - c) Fixieren Sie den Standfuß durch Festdrehen der Kontermutter [A].
 - d) Falls erforderlich, wiederholen Sie die Schritte a bis c für weitere Standfüße, bis die Basisbox gerade steht und der Mindestabstand eingehalten wird.



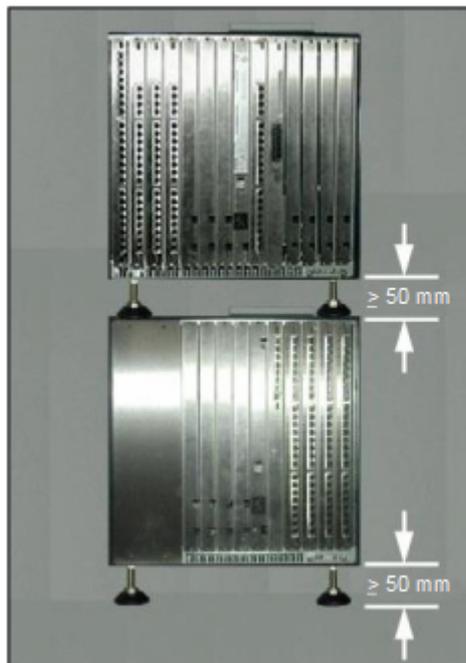
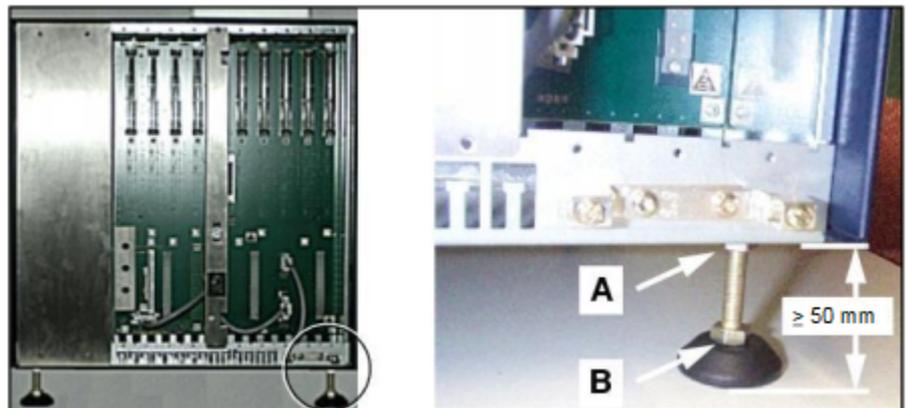
- 4) Stellen Sie die Erweiterungsbox auf die Basisbox.

Die Standfüße der Systemboxen sind mit Vertiefungen versehen. Achten Sie beim Aufstellen der Erweiterungsbox darauf, dass diese Vertiefungen genau auf die Schraubenköpfe in den vier Ecken der Basisbox platziert werden.



- 5) Prüfen Sie, ob der Mindestabstand von 50 mm zwischen Erweiterungsbox und Basisbox nicht unterschritten wird.

- 6) Falls erforderlich, richten Sie die Erweiterungsbox folgendermaßen aus:
- Lösen Sie die Kontermutter [A] eines Standfußes mit Hilfe eines Gabelschlüssels (Schlüsselweite = 13 mm).
 - Ändern Sie die Höhe des Standfußes durch Drehen der Schraubmutter [B] so, dass die Erweiterungsbox gerade auf der Basisbox steht und der Mindestabstand eingehalten wird.
 - Fixieren Sie den Standfuß durch Festdrehen der Kontermutter [A].
 - Falls erforderlich, wiederholen Sie die Schritte a bis c für weitere Standfüße, bis die Erweiterungsbox gerade steht und der Mindestabstand zur Basisbox eingehalten wird.



7.1.1.3 Zweiboxsystem: Wie Sie die Systemboxen nebeneinander aufstellen

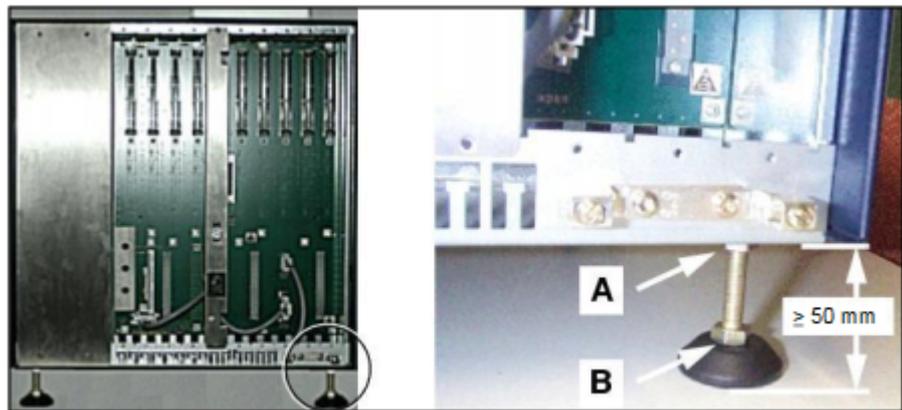
Voraussetzungen

Die Voraussetzungen für die Auswahl des Montagestandorts bei freistehender Montage wurden berücksichtigt (siehe [Voraussetzungen für die Installation](#) auf Seite 31).

Die vordere und hintere Kunststoffabdeckung der Systemboxen ist nicht montiert.

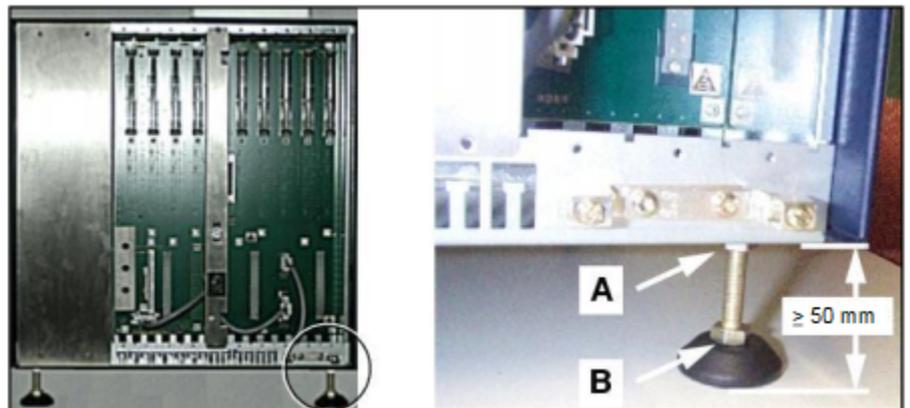
Schritt für Schritt

- 1) Platzieren Sie die Basisbox am Montageort und sorgen Sie für einen festen und ebenen Stand.
- 2) Prüfen Sie, ob der Mindestabstand von 50 mm zwischen Unterkante der Basisbox und Boden nicht unterschritten wird.
- 3) Falls erforderlich, richten Sie die Basisbox folgendermaßen aus:
 - a) Lösen Sie die Kontermutter [A] eines Standfußes mit Hilfe eines Gabelschlüssels (Schlüsselweite = 13 mm).
 - b) Ändern Sie die Höhe des Standfußes durch Drehen der Schraubmutter [B] so, dass die Basisbox gerade steht und der Mindestabstand eingehalten wird.
 - c) Fixieren Sie den Standfuß durch Festdrehen der Kontermutter [A].
 - d) Falls erforderlich, wiederholen Sie die Schritte a bis c für weitere Standfüße, bis die Basisbox gerade steht und der Mindestabstand eingehalten wird.



- 4) Stellen Sie die Erweiterungsbox neben die Basisbox.
- 5) Prüfen Sie, ob der Mindestabstand von 50 mm zwischen Unterkante der Erweiterungsbox und Boden nicht unterschritten wird.

- 6) Falls erforderlich, richten Sie die Erweiterungsbox folgendermaßen aus:
- Lösen Sie die Kontermutter [A] eines Standfußes mit Hilfe eines Gabelschlüssels (Schlüsselweite = 13 mm).
 - Ändern Sie die Höhe des Standfußes durch Drehen der Schraubmutter [B] so, dass die Erweiterungsbox gerade steht und der Mindestabstand eingehalten wird.
 - Fixieren Sie den Standfuß durch Festdrehen der Kontermutter [A].
 - Falls erforderlich, wiederholen Sie die Schritte a bis c für weitere Standfüße, bis die Erweiterungsbox gerade steht und der Mindestabstand eingehalten wird.



7.1.2 19"-Schrankmontage

OpenScape Business X8 ist ein modulares Kommunikationssystem, das als Einboxsystem (Basisbox) oder als Zweiboxsystem (Basisbox + Erweiterungsbox) in einem 19"-Schrank montiert werden kann.

7.1.2.1 So montieren Sie eine Systembox in einem 19-Zoll-Rack

Voraussetzungen

Die Voraussetzungen für die Auswahl des Montagestandorts für die 19-Zoll-Rackmontage wurden berücksichtigt (siehe [Voraussetzungen für die Installation](#) auf Seite 31).

Hardwareinstallation von OpenScape Business X8

Die vorderen und hinteren Kunststoffabdeckungen sind nicht an der Systembox befestigt.

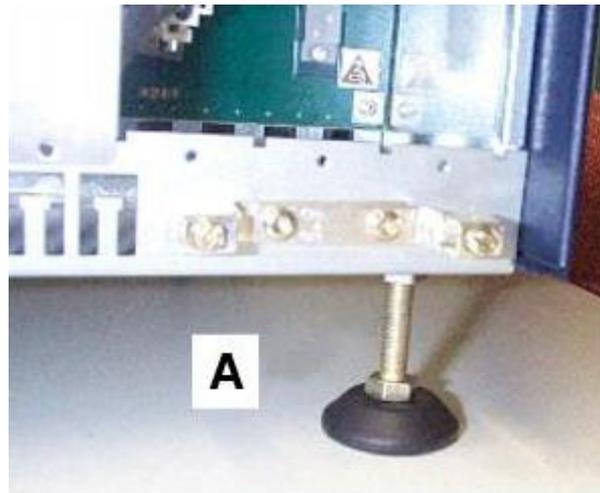
Zwei schrankspezifische Halterungen (mit einer Höchstlast von > 40 kg) sind vorhanden. Diese müssen vom Lieferanten des 19-Zoll-Schranks gestellt werden).

Anmerkung: Die Verwendung von Schrankböden ist nicht zulässig, um eine Überhitzung zu verhindern.

Die für die Befestigung von Stütz- und Winkelhalterungen am 19-Zoll-Rack benötigten schrankspezifischen Schrauben sind vorhanden.

Schritt für Schritt

- 1) Entfernen Sie die vier Füße der Systembox:
 - a) Schrauben Sie die Kontermutter [A] auf einem der Füße mit einem Gabelschlüssel (Weite = 13 mm) ab.
 - b) Schrauben Sie den Fuß vollständig ab.
 - c) Wiederholen Sie die Schritte a und b für die restlichen drei Gehäusefüße.



- 2) Befestigen Sie die beiden mitgelieferten Winkelhalterungen [B] mithilfe der beigelegten Schrauben an den Seiten der Systembox.

- 3) Befestigen Sie die rechte und linke Stützhalterung [C] mithilfe der beigelegten Schrauben am 19-Zoll-Rack.



- 4) Heben Sie die Systembox in das 19-Zoll-Rack und positionieren Sie es auf den beiden Stützhalterungen [C]. Schieben Sie die Systembox in das 19-Zoll-Rack, bis die Vorderkante der Systembox mit der Vorderseite des 19-Zoll-Rahmens bündig ist.



ACHTUNG: Allgemeine Verletzungs- bzw. Unfallgefahr am Arbeitsplatz

Versuchen Sie niemals, eine Systembox ohne Hilfe in ein 19-Zoll-Rack zu heben.

- 5) Verwenden Sie die zwei Winkelhalterungen [B] und die mitgelieferten Schrauben, um die Systembox am 19-Zoll-Rack zu befestigen.
- 6) Wiederholen Sie die Schritte 1 bis 6, wenn Sie eine Erweiterungsbox installieren möchten.

7.2 Patch-Panel (optional)

Für eine 19-Zoll-Rackmontage des OpenScape Business X8 Kommunikationssystems können die Telefone, Amtsleitungen usw. über das externe Patch-Panel angeschlossen werden.

Patch-Panel S30807-K6143-X

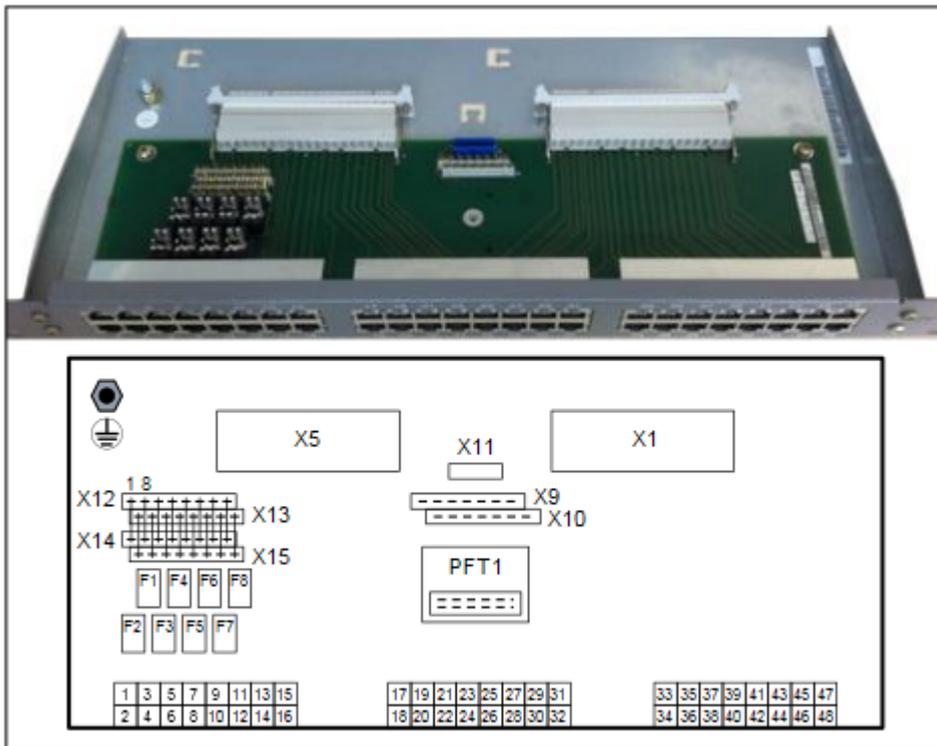


Abbildung 13: Patch-Panel S30807-K6143-X

Wesentliche Merkmale

- Zwei SIVAPAC-Anschlüsse (X1, X5) für den Anschluss an die Backplane des Kommunikationssystems über CABLUs (werkseitig vorgefertigte Verkabelungseinheiten)
- Mithilfe von Jumper-Kabeln müssen die Klemmleisten X12 und X14 sowie X13 und X15 überbrückt werden. Der Kontakt zwischen dem SIVAPAC-Anschluss X5 und den ersten acht RJ45-Buchsen wird nur bei vorhandenen Kabelbrücken hergestellt.
- Beim direkten Überbrücken von Telefonen, Amtsleitungen usw. an den Klemmleisten X12 und X13 sind keine Kabelbrücken erforderlich.
- 48 RJ45-Buchsen (1 bis 48) für den Anschluss von Telefonen, Amtsleitungen usw.

Tabelle 1: Patch-Panel S30807-K6143-X - Belegung der RJ45-Buchsen

Pin	Signal
4	a
5	b

Die RJ45-Buchsen sind jeweils zweiadrig belegt.

- Acht Steckplätze für Überspannungsableiter (ÜSAG) (F1 bis F8)

Anmerkung:

Brandgefahr durch Überspannung

Bei Leitungslängen über 500 m und bei Leitungen, die das Gebäude verlassen, müssen die Module für die analogen und digitalen Teilnehmerleitungen durch einen externen Blitzschutz geschützt werden.

Ein solcher Blitzschutz wird als zusätzlicher Primärschutz bezeichnet. Der zusätzliche Primärschutz wird durch die Installation von ÜSAGs (gasgefüllte Überspannungsableiter) im Patch-Panel gewährleistet.

Tipp: X9, X10, X11 und PFT1 sind nicht für die Verwendung mit OpenScape Business gedacht.

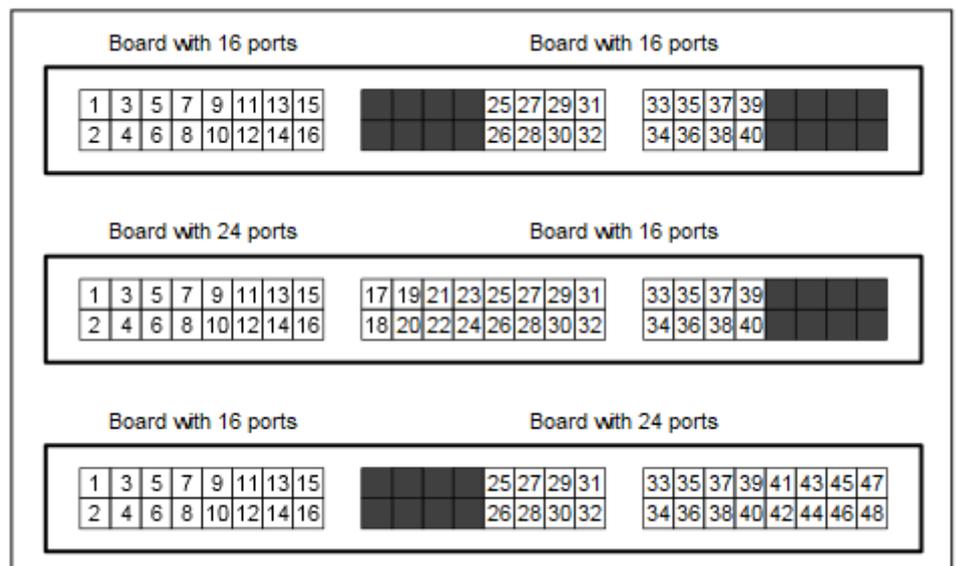


Abbildung 14: Patch-Panel S30807-K6143-X – Verwendung der 48 RJ45-Buchsen

Die obige Abbildung zeigt die Verwendung der 48 RJ45-Buchsen in Abhängigkeit je nach Anzahl der Schnittstellen der angeschlossenen Peripheriebaugruppen.

S₀ Patch-Panel C39104-Z7001-B3

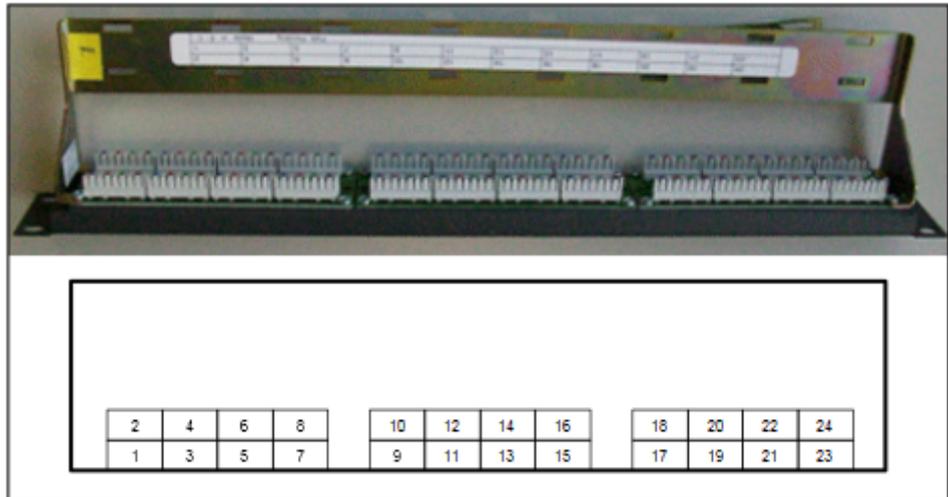


Abbildung 15: S₀ Patch-Panel C39104-Z7001-B3

Wesentliche Merkmale

- 24 RJ45-Buchsen (1 bis 24) für den Anschluss von ISDN-Telefonen, ISDN-Amtsleitungen usw.

Der Anschluss der Backplane des Kommunikationssystems erfolgt manuell über Open-End-Kabel, die manuell am S₀-Patch-Panel befestigt werden müssen.

Tabelle 2: S₀-Patch-Panel C39104-Z7001-B3 - Belegung der RJ45-Buchsen

Pin	Signal	
	Amtsanschluss/ Vernetzung	Teilnehmeranschluss
3	Senden +	Empfangen +
4	Empfangen +	Senden +
5	Empfangen –	Senden –
6	Senden –	Empfangen –

Jede RJ45-Buchse muss vier Adern aufweisen.

Anmerkung: Wenn Sie Patch-Panels eines Drittanbieters verwenden, müssen Sie die Anweisungen des Herstellers zur Installation und Schutzerdung beachten.

7.2.1 Wie Sie ein Patch-Panel in einen 19"-Schrank montieren

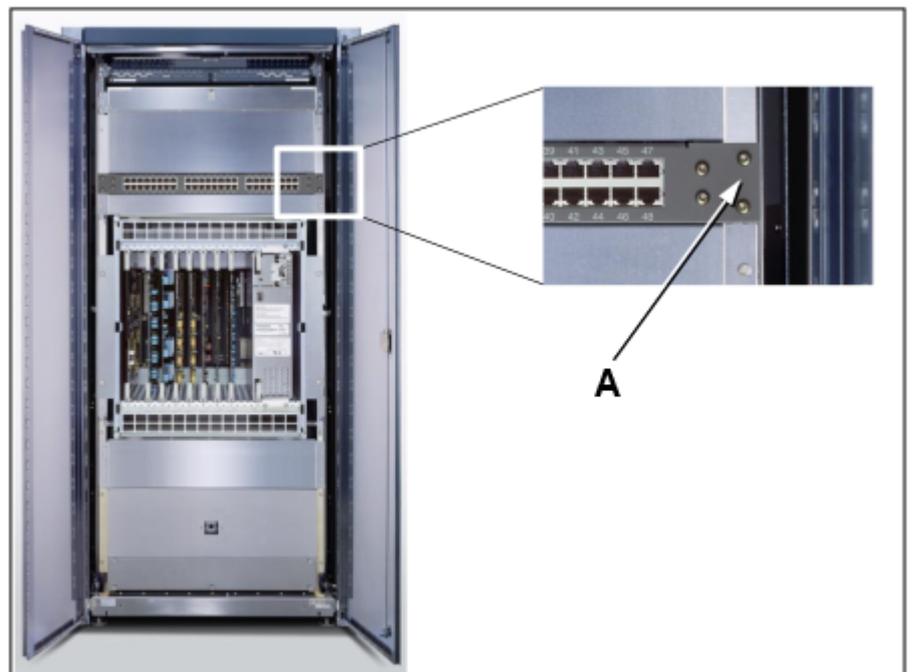
Voraussetzungen

Die Voraussetzungen für die Auswahl des Montagestandorts bei 19"-Schrankmontage wurden berücksichtigt (siehe [Voraussetzungen für die Installation](#) auf Seite 31).

Schrankspezifische Schrauben für die Befestigung des Patch-Panels am 19"-Schrank stehen zur Verfügung.

Schritt für Schritt

Heben Sie das Patch-Panel in den 19"-Schrank und befestigen Sie dieses mit den dafür vorgesehenen Schrauben [A] am 19"-Schrank.



7.3 Schutzerdung

Mit der Schutzerdung wird eine sichere Verbindung zum Erdpotential hergestellt, um bei Auftreten eines Fehlers vor gefährlich hohen Berührungsspannungen zu schützen.



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

- Schutzerden Sie die Systemboxen des Kommunikationssystems OpenScape Business X8 und eventuell verwendete Hauptverteiler und Patch-Panels durch separate Schutzleiter. Verbinden Sie die Systemboxen Ihres Kommunikationssystems, Ihren Hauptverteiler und Ihre Patch-Panels vor Inbetriebnahme und Anschluss der Telefone und Leitungen ordnungsgemäß mit dem Schutzleiter.

- Achten Sie auf eine geschützte Verlegung und Zugentlastung der Schutzleiter (Mindest-Leiterquerschnitt = 12 AWG/2,5 mm²). Können äußere Einflüsse auf einen Schutzleiter einwirken und ist eine geschützte Verlegung nicht möglich, ist für den Schutzleiter ein Leiterquerschnitt von 10 AWG/4 mm² erforderlich.
-

7.3.1 Schutzerdung bei freistehender Montage

Die Schutzerdung der Systemboxen des Kommunikationssystems und der eventuell verwendeten Hauptverteiler erfolgt zum Beispiel über die Potentialausgleichsschiene des Gebäudes, über eine Haupt-Erdsammelschiene oder über ein Erdungsfeld.

7.3.1.1 So nehmen Sie für Schutzerdung des Hauptverteilers MDFU vor

Voraussetzungen

Ein Masseanschluss mit einem Widerstand von weniger als 2 Ohm ist vorhanden ist. Beispiele: Potentialausgleichsleiste des Gebäudes, Hauptersammelschiene, Erdungsfeld



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.



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

- Schutzerden Sie die Systemboxen des OpenScape Business X8 Kommunikationssystems und möglichst alle verwendeten Hauptverteiler durch separate Schutzleiter. Schließen Sie die Systemboxen Ihres Kommunikationssystems und Ihren Hauptverteiler an den Schutzleiter an, bevor Sie das System in Betrieb nehmen und Telefone und Leitungen anschließen.
 - Achten Sie darauf, dass die Schutzleiter geschützt und zugentlastet sind (Mindestleiterquerschnitt = 12 AWG/2,5 mm²). Ein Leiterquerschnitt von mindestens 10 AWG/4 mm² ist erforderlich, um die Auswirkungen externer Faktoren zu blockieren, wenn der Schutzleiter nicht geschützt werden kann.
-

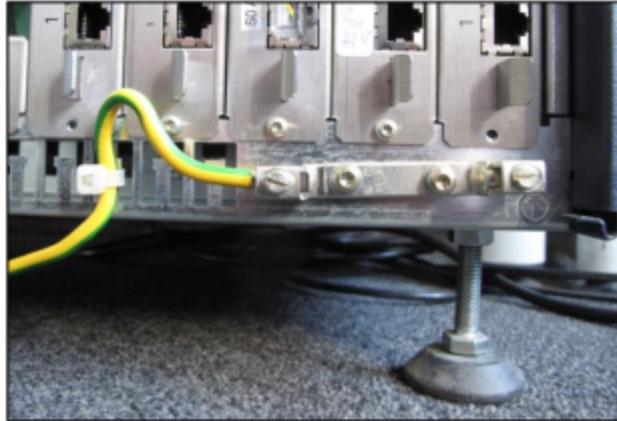
Die Erdung der Systemboxen muss von einem Erdungspunkt in einer Sternkonfiguration erfolgen.

Die in IEC 60364, IEC 60950-1 und IEC 62368-1 angegebenen Ausführungsbestimmungen müssen bei der Installation eingehalten werden.

Gehen Sie wie folgt vor, um die Schutzerdung sicherzustellen:

Schritt für Schritt

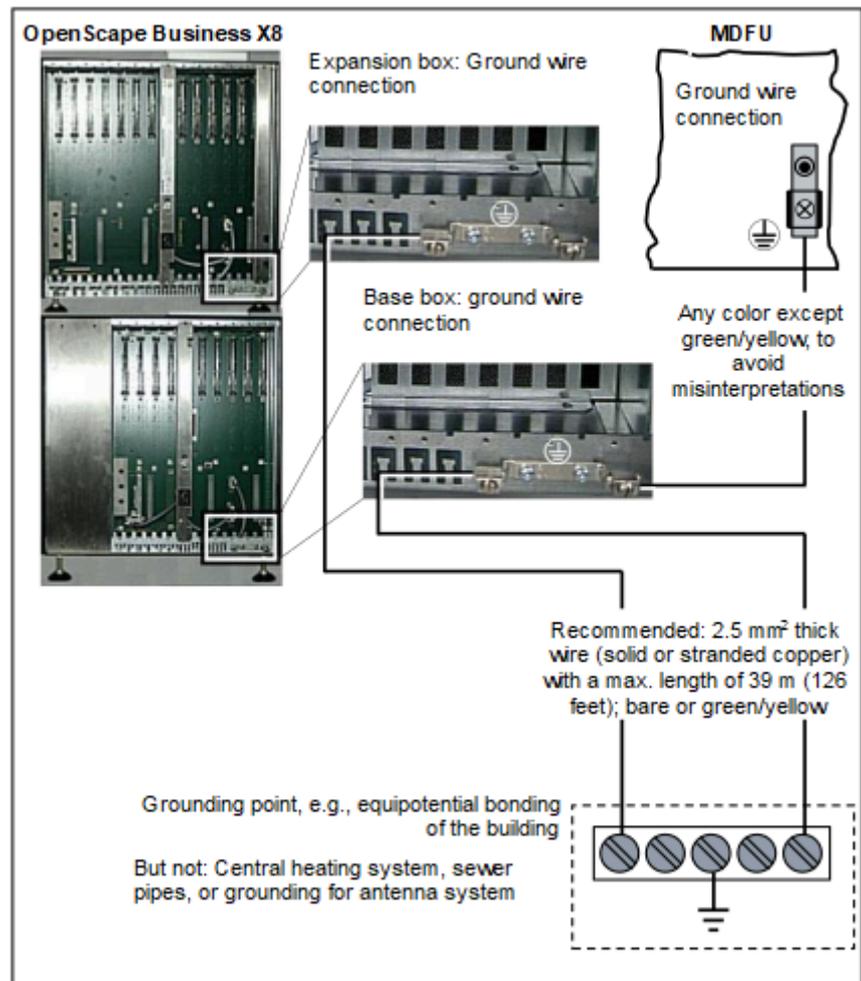
- 1) Befestigen Sie einen separaten Schutzleiter wie in der folgenden Abbildung dargestellt an der Erdungsklemme der Basisbox des Kommunikationssystems.



- 2) Sorgen Sie für die Zugentlastung des Schutzleiters, indem Sie ihn mit einem Kabelbinder an der Basisbox befestigen.
- 3) Verwenden Sie für den Anschluss der Erdungsklemme der Basisbox an die Erdungsklemme des externen Hauptverteilers MDFU einen Leiter mit einer Stärke von 12 AWG/2,5 mm² (ein- oder mehrdrähtiges Kupfer) mit einer maximalen Länge von 39 Metern. Verwenden Sie alle Farben außer grün/gelb, um mögliche Verwechslungen zu vermeiden.
- 4) Wenn eine Erweiterungsbox vorhanden ist: Befestigen Sie einen separaten Schutzleiter an der Erdungsklemme der Erweiterungsbox des Kommunikationssystems.
- 5) Wenn eine Erweiterungsbox vorhanden ist: Sorgen Sie für die Zugentlastung des Schutzleiters, indem Sie ihn mit einem Kabelbinder an der Erweiterungsbox befestigen.
- 6) Wählen Sie eine der folgenden Optionen:
 - **Nicht für USA und Kanada:** Verbinden Sie den oder die separaten Schutzleiter der Systembox(en) mit dem Erdungspunkt (z. B. die Potenzialausgleichsleiste des Gebäudes), wie im Schaltdiagramm in der

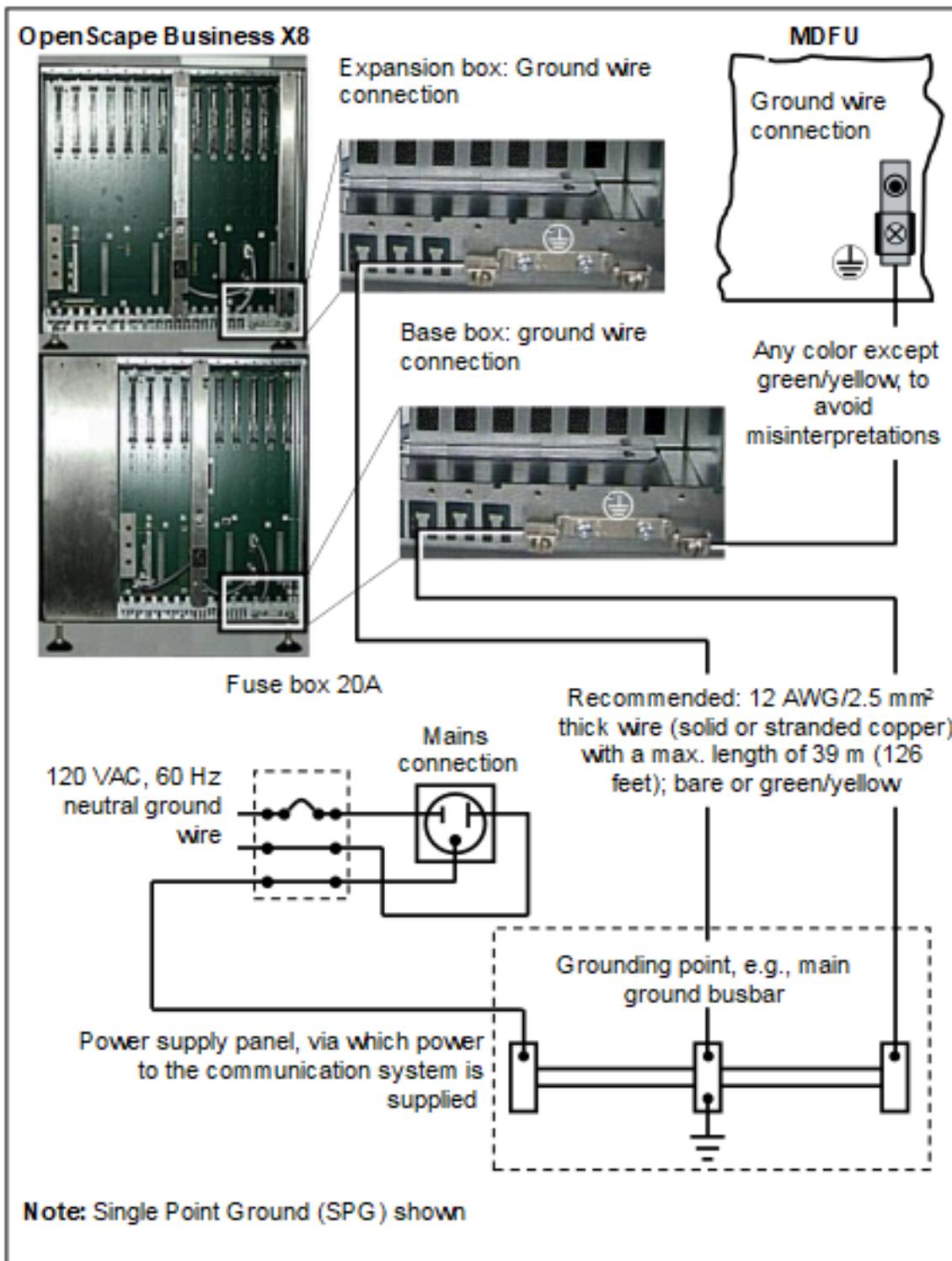
Hardwareinstallation von OpenScape Business X8

folgenden Abbildung dargestellt. Achten Sie darauf, dass alle verlegten Schutzleiter geschützt und zugentlastet sind.



- **Nur für USA und Kanada:** Verbinden Sie den oder die separaten Schutzleiter der Systembox(en) mit dem Erdungspunkt (z. B. die Haupterdsammelschiene, Erdungsfeld), wie im Schaltdiagramm in der

folgenden Abbildung dargestellt. Achten Sie darauf, dass alle verlegten Schutzleiter geschützt und zugentlastet sind.



7.3.1.2 Wie Sie die Schutzerdung prüfen

Voraussetzungen

Die Systembox oder Systemboxen des Kommunikationssystems sind noch nicht über Netzanschlusskabel mit dem Niederspannungsnetz verbunden.

Die separate Schutzerdung für jede einzelne Systembox des Kommunikationssystems und für den oder die verwendeten Hauptverteiler ist angeschlossen.

Führen Sie vor der Inbetriebnahme den folgenden Test durch, um die ordnungsgemäße Schutzerdung des Kommunikationssystems und der verwendeten Hauptverteiler sicherzustellen.

Schritt für Schritt

- 1) Prüfen Sie den Ohmschen Widerstand der Schutzleiterverbindung zum Kommunikationssystem:

Die Messung erfolgt zwischen dem Schutzkontakt einer Schuko-Steckdose der Hausinstallation (am Anschlussort des Kommunikationssystems) und einer Systembox des Kommunikationssystems.

- 2) Wiederholen Sie die Messung für alle weiteren Systemboxen des Kommunikationssystems.

- 3) Prüfen Sie den Ohmschen Widerstand zwischen den Systemboxen des Kommunikationssystems und dem oder den Hauptverteilern.

Das Ergebnis (Sollwert) einer Messung muss wesentlich kleiner als 10 Ohm betragen.

Sollten Sie bei einer Messung zu einem anderen Ergebnis kommen, beauftragen Sie einen qualifizierten Elektrotechniker. Dieser muss den Potentialausgleich der Hausinstallation prüfen und die Niederohmigkeit der Schutzleiterverbindung sicherstellen.

7.3.2 Schutzerdung bei 19"-Schrankmontage

Die Schutzerdung der Systemboxen des Kommunikationssystems und der eventuell verwendeten Patch-Panels erfolgt über die Potentialausgleichsschiene des 19"-Schranks.

7.3.2.1 So stellen Sie eine Schutzerdung für das Kommunikationssystem und das Patch-Panel her

Voraussetzungen

Ein Masseanschluss mit einem Widerstand von weniger als 2 Ohm ist vorhanden ist. Beispiele: Potentialausgleichsleiste des Gebäudes, Hauptersammelschiene, Erdungsfeld

Das 19-Zoll-Rack wird mit einem separaten Schutzleiter (grün/gelb) geerdet. Das 19-Zoll-Rack ist mit einer Potentialausgleichsleiste ausgestattet, an dem

die Systemboxen der Kommunikationssysteme und die Patch-Panels separat geerdet werden können.



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.



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

- Schutzerden Sie die Systemboxen des OpenScape Business X8 Kommunikationssystems und möglichst alle Patch-Panels durch separate Schutzleiter. Schließen Sie die Systemboxen Ihres Kommunikationssystems und Ihre Patch-Panels an den Schutzleiter an, bevor Sie das System in Betrieb nehmen und Telefone und Leitungen anschließen.
 - Achten Sie darauf, dass die Schutzleiter geschützt und zugentlastet sind (Mindestleiterquerschnitt = 12 AWG/2,5 mm²). Ein Leiterquerschnitt von mindestens 10 AWG/4 mm² ist erforderlich, um die Auswirkungen externer Faktoren zu blockieren, wenn ein Schutzleiter nicht geschützt werden kann.
-

Die Erdung der Systemboxen muss von einem Erdungspunkt in einer Sternkonfiguration erfolgen.

Die in IEC 60364, IEC 60950-1 und IEC 62368-1 angegebenen Ausführungsbestimmungen müssen bei der Installation eingehalten werden.

Anmerkung:

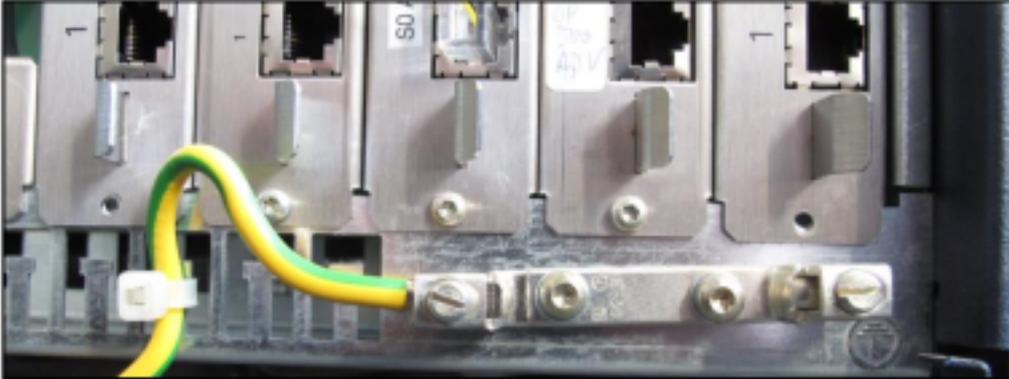
Die aufgeführten Anforderungen gelten bei der Verwendung von Patch-Panels eines anderen Herstellers.

Eine Schutzerdung des S₀-Patch-Panels (C39104-Z7001-B3) ist nicht erforderlich.

Gehen Sie wie folgt vor, um die Schutzerdung sicherzustellen:

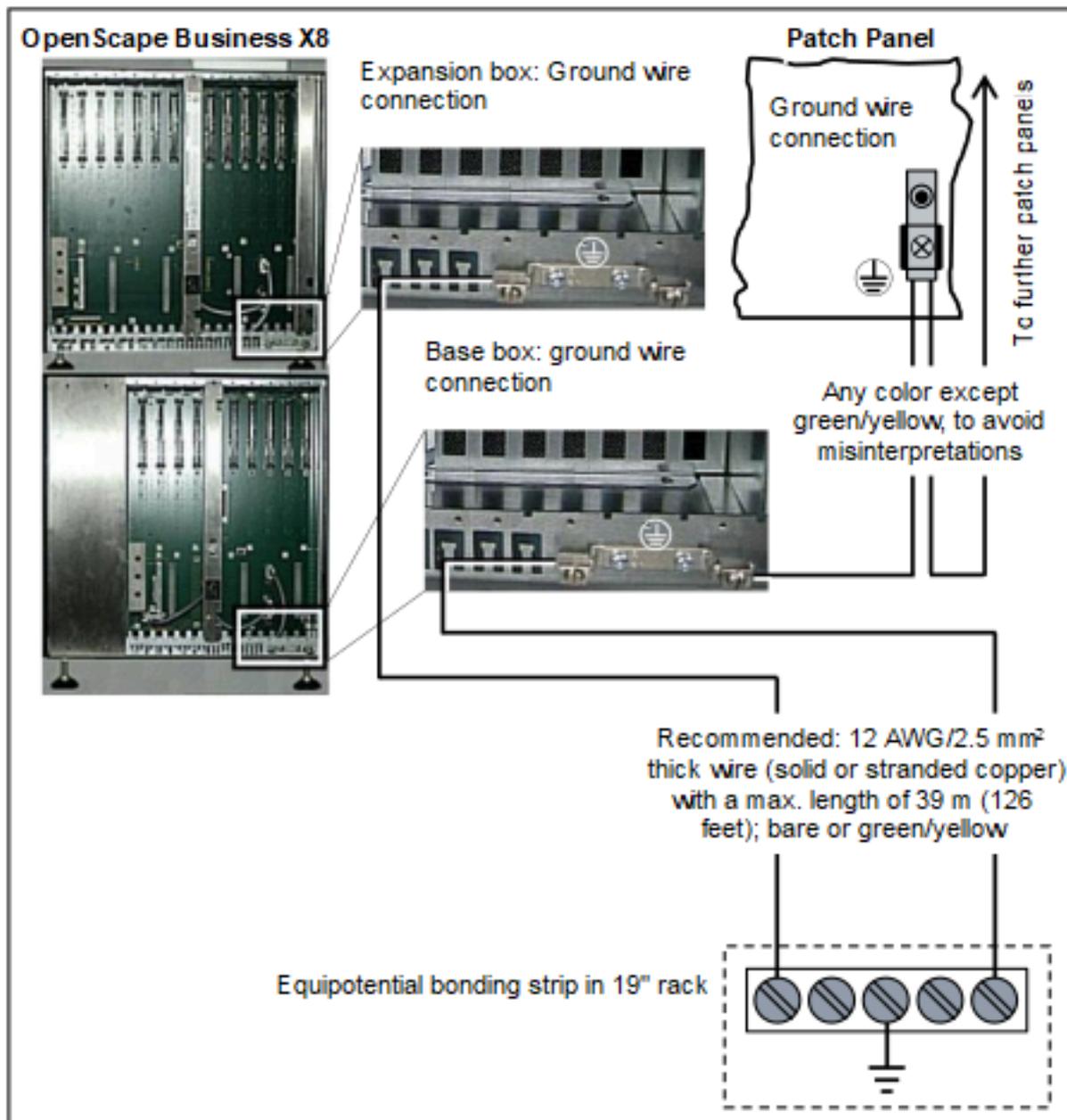
Schritt für Schritt

- 1) Befestigen Sie einen separaten Schutzleiter wie in der folgenden Abbildung dargestellt an der Erdungsklemme der Basisbox des Kommunikationssystems.



- 2) Sorgen Sie für die Zugentlastung des Schutzleiters, indem Sie ihn mit einem Kabelbinder an der Basisbox befestigen.
- 3) Verwenden Sie für den Anschluss der Erdungsklemme der Basisbox an die Erdungsklemme des Patch-Panels (S30807-K6143-X) einen Leiter mit einer Stärke von 12 AWG/2,5 mm² (ein- oder mehrdrähtiges Kupfer) mit einer maximalen Länge von 39 Metern. Verwenden Sie alle Farben außer grün/gelb, um mögliche Verwechslungen zu vermeiden.
- 4) Wenn ein weiteres Patch-Panel (S30807-K6143-X) vorhanden ist: Verwenden Sie für den Anschluss der Erdungsklemmen der Patch-Panels miteinander einen Leiter mit einer Stärke von 12 AWG/2,5 mm² (ein- oder mehrdrähtiges Kupfer) mit einer maximalen Länge von 39 Metern. Verwenden Sie alle Farben außer grün/gelb, um mögliche Verwechslungen zu vermeiden.
- 5) Wenn eine Erweiterungsbox vorhanden ist: Befestigen Sie einen separaten Schutzleiter an der Erdungsklemme der Erweiterungsbox des Kommunikationssystems.
- 6) Wenn eine Erweiterungsbox vorhanden ist: Sorgen Sie für die Zugentlastung des Schutzleiters, indem Sie ihn mit einem Kabelbinder an der Erweiterungsbox befestigen.
- 7) Verbinden Sie den oder die separaten Schutzleiter der Systembox(en) mit der Potenzialausgleichsleiste im 19-Zoll-Rack, wie im Schaltdiagramm in

der folgenden Abbildung dargestellt. Achten Sie darauf, dass alle verlegten Schutzleiter geschützt und zugentlastet sind.



7.3.2.2 Wie Sie die Schutzerdung prüfen

Voraussetzungen

Die Systembox oder Systemboxen des Kommunikationssystems und alle weiteren Geräte im 19"-Schrank sind nicht über Netzanschlusskabel mit dem Niederspannungsnetz verbunden.

Die separate Schutzerdung für jede einzelne Systembox des Kommunikationssystems und für den oder die verwendeten Patch-Panels ist angeschlossen.

Der 19"-Schrank ist durch einen separaten Schutzleiter (grün/gelb) geschützt.

Führen Sie vor der Inbetriebnahme den folgenden Test durch, um die ordnungsgemäße Schutzterdung des Kommunikationssystems und der verwendeten Patch-Panels sicherzustellen.

Schritt für Schritt

- 1)** Prüfen Sie den Ohmschen Widerstand der Schutzleiterverbindung zum Kommunikationssystem:
 - a) Die erste Messung erfolgt zwischen dem Schutzkontakt einer Schuko-Steckdose der Hausinstallation und der Potentialausgleichsschiene im 19"-Schrank.
 - b) Die zweite Messung erfolgt zwischen der Potentialausgleichsschiene im 19"-Schrank und einer Systembox des Kommunikationssystems.
 - c) Wiederholen Sie die zweite Messung für alle weiteren Systemboxen des Kommunikationssystems.
- 2)** Prüfen Sie den Ohmschen Widerstand zwischen den Systemboxen des Kommunikationssystems und dem oder den Patch-Panels.

Das Ergebnis (Sollwert) einer Messung muss wesentlich kleiner als 10 Ohm betragen.

Sollten Sie bei einer Messung zu einem anderen Ergebnis kommen, beauftragen Sie einen qualifizierten Elektrotechniker. Dieser muss den Potentialausgleich der Hausinstallation prüfen und die Niederohmigkeit der Schutzleiterverbindung sicherstellen.

7.4 Konfigurationshinweise

Die Konfigurationshinweise enthalten Informationen über die Steckplätze in der Basisbox und in der Erweiterungsbox, die Initialisierung der Baugruppen, die Verteilung der PCM-Highways in der Basisbox und in der Erweiterungsbox sowie zur Erweiterungsbox und zur Baugruppeninstallation.

7.4.1 Baugruppensteckplätze in der Basisbox

Die Basisbox verfügt über neun Steckplätze für Peripheriebaugruppen (Steckplätze 1 bis 5 und 7 bis 10). Ein fixer Steckplatz ist für das OCCL- oder OCCLA-Mainboard vorgesehen (Steckplatz 6). Je nach Bedarf kann die Stromversorgung LUNA2 bis zu dreimal in der Erweiterungsbox eingesetzt werden.

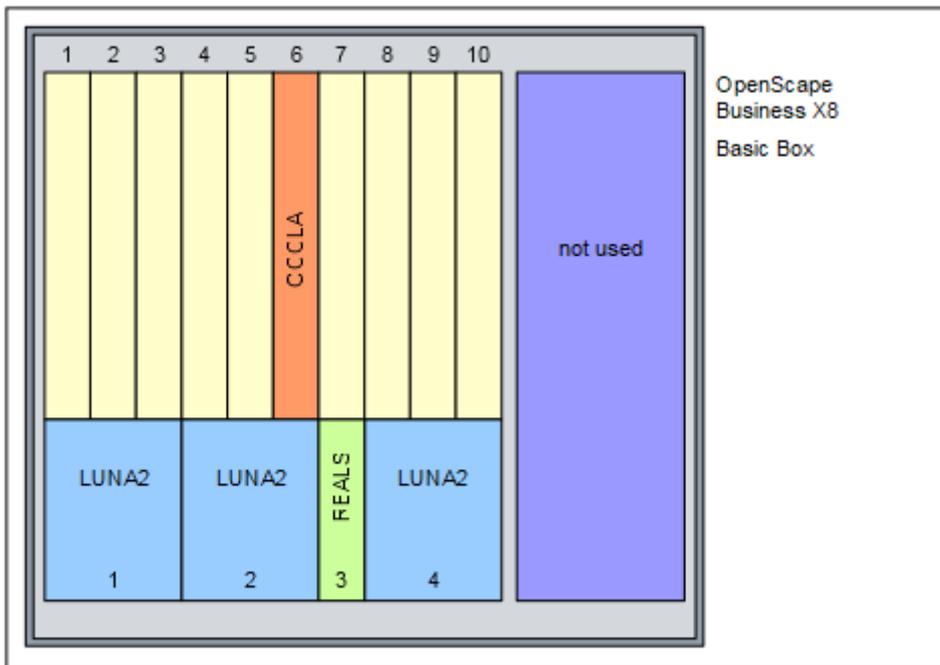


Abbildung 16: OpenScape Business X8 – Baugruppensteckplätze in der Basisbox

7.4.2 Baugruppen-Steckplätze in der Erweiterungsbox

In der Erweiterungsbox stehen dreizehn Steckplätze für Peripheriebaugruppen zur Verfügung (Steckplätze 1 bis 6 und 8 bis 14). Je nach Bedarf kann die Stromversorgung LUNA2 bis zu viermal in der Erweiterungsbox eingesetzt werden.

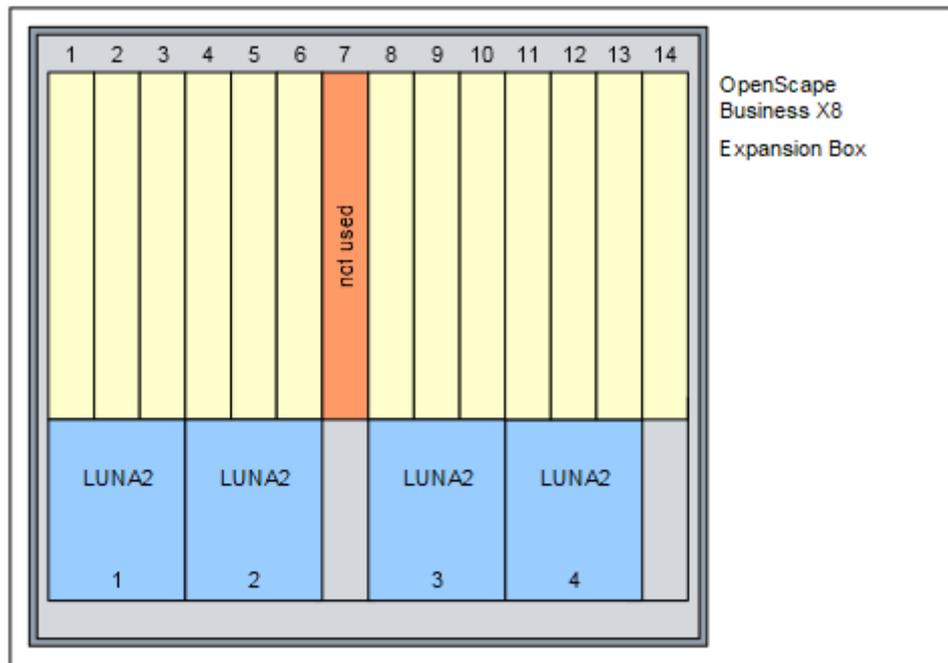


Abbildung 17: OpenScape Business X8 – Baugruppen-Steckplätze in der Erweiterungsbox

7.4.3 Spezielle Baugruppensteckplätze

Die folgenden Baugruppen werden in speziellen Steckplätzen verwendet.

DBSAP

Die DBSAP-Baugruppe ist im Lieferumfang der Erweiterungsbox enthalten und wird werkseitig mit dem entsprechenden Backplane-Stecker der Erweiterungsbox verbunden.

LUNA2

Die Steckplätze für die LUNA2 befinden sich im unteren Teil des Baugruppenrahmens einer Systembox. In der Basisbox stehen drei Steckplätze und in der Erweiterungsbox vier Steckplätze zur Verfügung.

Anmerkung:

LUNA2 darf nur im spannungslosen Zustand gesteckt oder gezogen werden (Schalterstellung = DC#OFF).

Vor der Inbetriebnahme des Kommunikationssystems müssen die Steckplätze der Stromversorgung durch Sonnenblenden abgedeckt werden.

REALS

Der Steckplatz für die REALS befindet sich im unteren Teil des Baugruppenrahmens der Basisbox.

Vor der Inbetriebnahme des Kommunikationssystems müssen die Steckplätze der Stromversorgungen und der Baugruppe REALS durch Sonnenblenden abgedeckt werden.

Weitere Informationen finden Sie in der entsprechenden Baugruppenbeschreibung.

7.4.4 Initialisierung der Baugruppen

Bei der Erstinbetriebnahme werden die Baugruppen beginnend vom der niedrigsten Einbauposition in aufsteigender Reihenfolge von der Systemsoftware erkannt und initialisiert.

Die Schnittstellen der Baugruppen werden gemäß der Pfeilrichtung in folgendem Bild in Betrieb genommen.

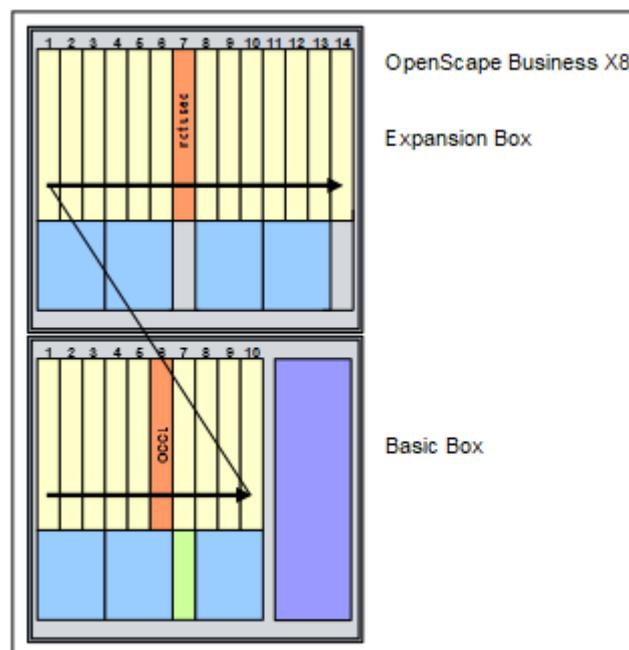


Abbildung 18: OpenScape Business X8 – Initialisierung der Baugruppen

Alle gesteckten Baugruppen gehen in Betrieb, wenn

- der Maximalausbau des Kommunikationssystems noch nicht erreicht ist.
Die Systemsoftware prüft beim sequentiellen Scannen der Einbauplätze, ob die maximale Anzahl von Teilnehmern oder Leitungen überschritten wird. Falls dies der Fall ist, bleibt die Baugruppe außer Betrieb.
- bei Amtsbaugruppen mindestens ein B-Kanal für den Einbauplatz verfügbar ist.

Es wird ausschließlich die Anzahl der verfügbaren B-Kanäle des Kommunikationssystems in Betrieb genommen.

7.4.5 Verteilung der PCM-Highways in der Basisbox

Die Basisbox stellt zwei PCM-Highway-Bündel mit jeweils 2 x 4 PCM-Highways für die Peripheriebaugruppen-Steckplätze bereit. Pro PCM-Highway stehen

Hardwareinstallation von OpenScape Business X8

32 Zeitmultiplexkanäle zur Verfügung. Sind diese belegt, können keine weiteren Gesprächsaufträge mehr ausgeführt werden.

Um einen blockierungsfreien Betrieb zu gewährleisten, ist bei der Baugruppenbestückung darauf zu achten, dass die Peripheriebaugruppen auf einem PCM-Abschnitt nicht mehr als die zur Verfügung stehenden Zeitmultiplexkanäle erfordern.

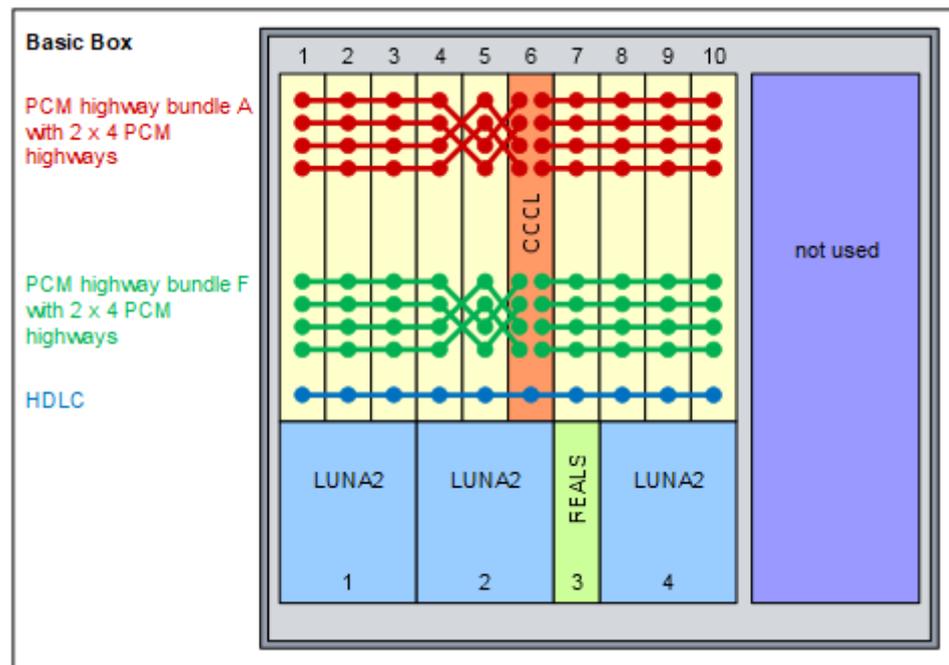


Abbildung 19: OpenScape Business X8 – PCM-Highways in der Basisbox

Die Nutzung der PCM-Highway-Bündel der Basisbox durch Peripheriebaugruppen erfolgt nach folgenden Regeln:

- Einboxsystem
 - PCM-Highway-Bündel A
 - Mit Ausnahme der Baugruppen DIUT2, DIUN2 und DIU2U nutzen die Peripheriebaugruppen ausschließlich die PCM-Highways des Bündels A.
 - 128 Zeitmultiplexkanäle (4 PCM-Highways) stehen auf dem PCM-Abschnitt für die Baugruppen-Steckplätze 1 bis 5 und auf dem PCM-Abschnitt für die Baugruppen-Steckplätze 7 bis 10 zur Verfügung.
 - PCM-Highway-Bündel F
 - Die Peripheriebaugruppen DIUT2, DIUN2 und DIU2U nutzen die PCM-Highways des Bündels F.
 - Für diese Baugruppen stehen damit 128 Zeitmultiplexkanäle auf dem PCM-Abschnitt für die Baugruppen-Steckplätze 1 bis 5 und auf dem PCM-Abschnitt für die Baugruppen-Steckplätze 7 bis 10 zur Verfügung.
 - Sind aufgrund der Bestückung mit diesen Baugruppen mehr als die 2 x 128 Zeitmultiplexkanäle des PCM-Highway-Bündel F erforderlich, greift das Kommunikationssystem automatisch auf Zeitmultiplexkanäle des PCM-Highway-Bündel A zurück. Allerdings werden nur komplette Baugruppen auf das andere Bündel geschaltet. Die verbleibenden restlichen Zeitmultiplexkanäle des PCM-Highway-Bündel F bleiben frei.

- Zweiboxsystem
 Alle Peripheriebaugruppen nutzen ausschließlich die PCM-Highways des Bündels A.

7.4.6 Verteilung der PCM-Highways in der Erweiterungsbox

Die Erweiterungsbox stellt ein PCM-Highway-Bündel mit 2 x 4 PCM-Highways für die Peripheriebaugruppen-Steckplätze bereit. Pro PCM-Highway stehen 32 Zeitmultiplexkanäle zur Verfügung. Sind diese belegt, können keine weiteren Gesprächsaufträge mehr ausgeführt werden.

Um einen blockierungsfreien Betrieb zu gewährleisten, ist bei der Baugruppenbestückung darauf zu achten, dass die Peripheriebaugruppen auf einem PCM-Abschnitt nicht mehr als die zur Verfügung stehenden Zeitmultiplexkanäle erfordern.

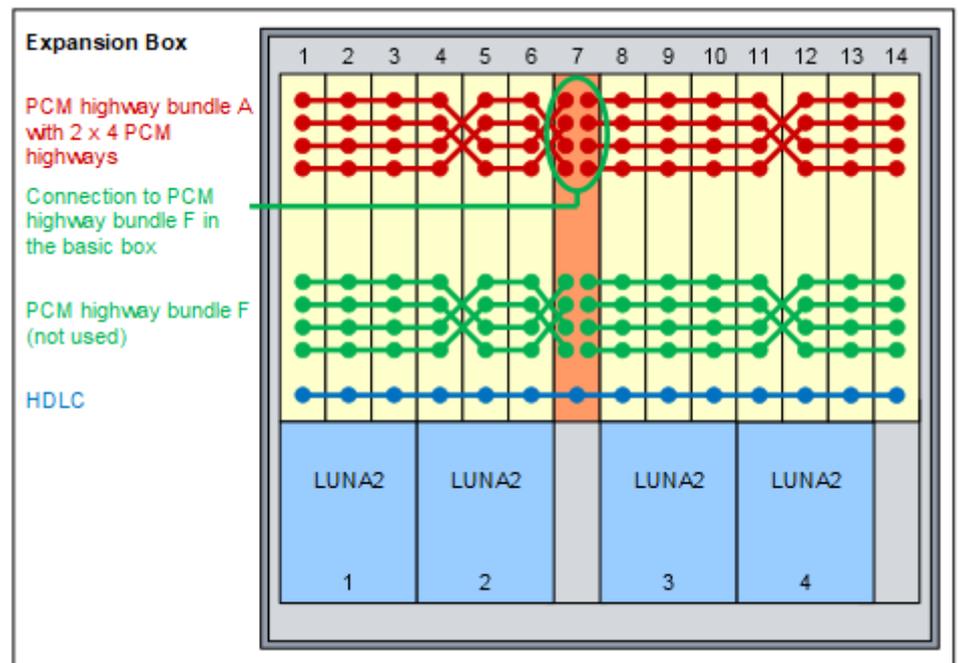


Abbildung 20: OpenScape Business X8 – PCM-Highways in der Erweiterungsbox

Alle Peripheriebaugruppen in der Erweiterungsbox nutzen ausschließlich die PCM-Highways des Bündels A.

128 Zeitmultiplexkanäle (4 PCM-Highways) stehen auf dem PCM-Abschnitt für die Baugruppen-Steckplätze 1 bis 6 und auf dem PCM-Abschnitt für die Baugruppen-Steckplätze 8 bis 14 zur Verfügung.

PCM-Highway-Bündel F wird nicht verwendet.

7.4.7 Zeitmultiplexkanäle der Peripheriebaugruppen

Für die Ausführung von Gesprächsaufträgen benötigen die Peripheriebaugruppen eine unterschiedliche Anzahl von Zeitmultiplexkanälen.

Diese Zeitmultiplexkanäle stellt OpenScape Business X8 über PCM-Highways zur Verfügung.

OpenScape Business X8 stellt PCM-Highway-Bündel mit jeweils 2 x 4 PCM-Highways für die Peripheriebaugruppen-Steckplätze bereit. Pro PCM-Highway stehen 32 Zeitmultiplexkanäle zur Verfügung. Sind diese belegt, können keine weiteren Gesprächsaufträge mehr ausgeführt werden. Um einen blockierungsfreien Betrieb des Kommunikationssystems zu gewährleisten, ist bei der Baugruppenbestückung darauf zu achten, dass die Peripheriebaugruppen auf einem PCM-Abschnitt nicht mehr als die zur Verfügung stehenden Zeitmultiplexkanäle erfordern.

Bei der Belegung von Zeitmultiplexkanälen durch die Peripheriebaugruppen wird unterschieden zwischen:

- Statischer Belegung

Bei Amts- und Querverkehrbaugruppen erfolgt eine statische Belegung der Zeitmultiplexkanäle. Damit wird sichergestellt, dass alle Anrufe verarbeitet werden können.

Anmerkung: Die Baugruppe TMDID nutzt ausschließlich die erste Hälfte eines PCM-Abschnitts. Damit stehen pro PCM-Abschnitt maximal 64 Kanäle für statische Zeitmultiplexkanäle der TMDID zur Verfügung. Um bei einem Einsatz der TMDID einen blockierungsfreien Betrieb des Kommunikationssystems zu gewährleisten, dürfen die auf einem PCM-Abschnitt eingesetzten Baugruppen nicht mehr als 64 statische Zeitmultiplexkanäle belegen.

Beispiele für einen PCM-Abschnitt:

2 x TMDID + 1 x DIU2U = 64 statische Zeitmultiplexkanäle = zulässige Bestückung

1 x TMDID + 1 x TMANI + 1 x DIUT2 = 76 statische Zeitmultiplexkanäle = unzulässige Bestückung

1 x TMDID + 2 x SLMO2 = 8 statische und 96 dynamische Zeitmultiplexkanäle = zulässige Bestückung

-
- Dynamischer Belegung

Bei Teilnehmerbaugruppen erfolgt eine dynamische Belegung der Zeitmultiplexkanäle. Die Kanäle werden mit jedem Anruf belegt und nach dem Gesprächsende wieder freigegeben. Die aktuelle Anzahl der erforderlichen Zeitmultiplexkanäle ist abhängig von der Anzahl der aktiven Teilnehmer.

- Statischer/dynamischer Belegung

Bei Baugruppen mit S_0 -Schnittstellen erfolgt die Belegung der Zeitmultiplexkanäle in Abhängigkeit von der Verwendung der einzelnen S_0 -Schnittstellen. Eine statische Belegung erfolgt bei Verwendung einer S_0 -Schnittstelle für den ISDN-Amtsanschluss (ISDN-Amt). Eine dynamische Belegung erfolgt bei Verwendung einer S_0 -Schnittstelle für den ISDN-Teilnehmeranschluss.

Informationen über die Anzahl der Zeitmultiplexkanäle, die die verschiedenen Peripheriebaugruppen benötigen, siehe *OpenScape Business X3/X5/X8 Servicedokumentation, Anhang - Hardware-Ausbau*.

7.4.8 Baugruppeninstallation

Peripheriebaugruppen können eingesetzt und entfernt werden, wenn die Stromversorgung angeschlossen ist (Hot-Swap-fähig). Verwenden Sie immer den Baugruppenschlüssel zum Entfernen und Einsetzen von Baugruppen.

Das Mainboard (OCCL oder OCCLA) darf nicht herausgezogen werden, wenn das System unter Spannung steht. In diesem Fall muss das System zuerst vom Stromnetz getrennt werden.

7.4.8.1 So setzen Sie eine Baugruppe ein

Voraussetzungen

Die vordere Kunststoffblende der Systembox ist nicht angebracht.

Ein freier Baugruppensteckplatz ist verfügbar.

Die Spezifikationen über die Verteilung der PCM-Highways in den Systemboxen wurden berücksichtigt.

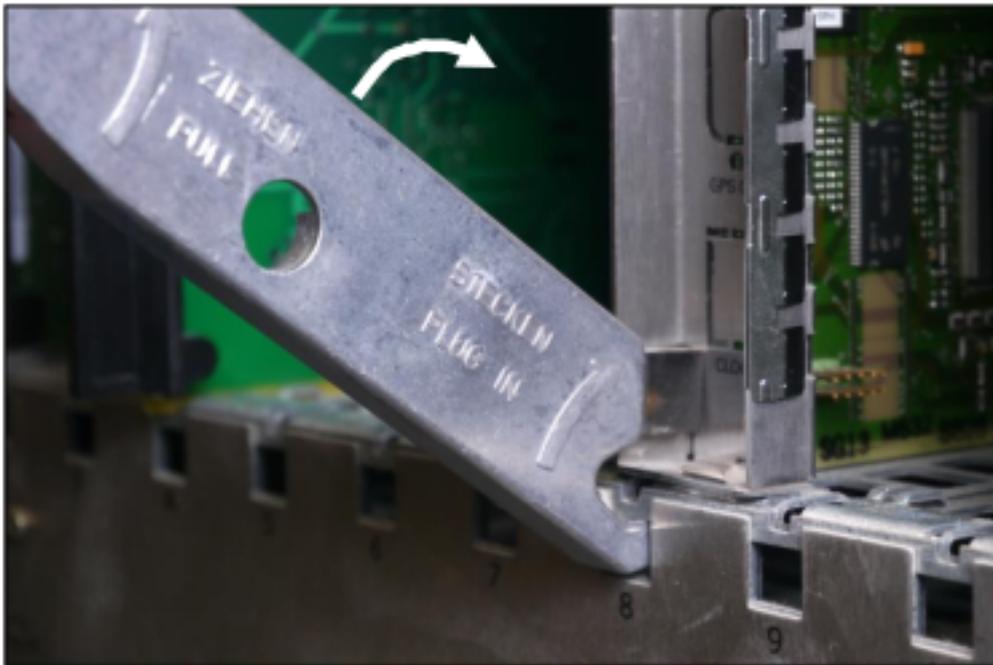
Anmerkung: Tragen Sie beim Umgang mit Baugruppen immer ein antistatisches Armband.

Die ESD-Maßnahmen zum Schutz elektrostatisch empfindlicher Geräte sind zu beachten und zu befolgen (siehe [Warnhinweise: Hinweis](#) auf Seite 16)

Schritt für Schritt

- 1) Schieben Sie die Baugruppe entlang der Führungsschienen bis zum Anschlag in die Systembox.
- 2) Stecken Sie die mit „Stecken / Plug In“ gekennzeichnete Spitze des Baugruppenschlüssels in die untere Aussparung der Frontblende der Baugruppe.

- 3) Hebeln Sie die Baugruppe in den Baugruppenrahmen der Systembox, indem Sie den Baugruppenschlüssel nach oben drücken.



7.4.8.2 So entfernen Sie eine Baugruppe

Voraussetzungen

Die vordere Kunststoffblende der Systembox ist nicht angebracht.

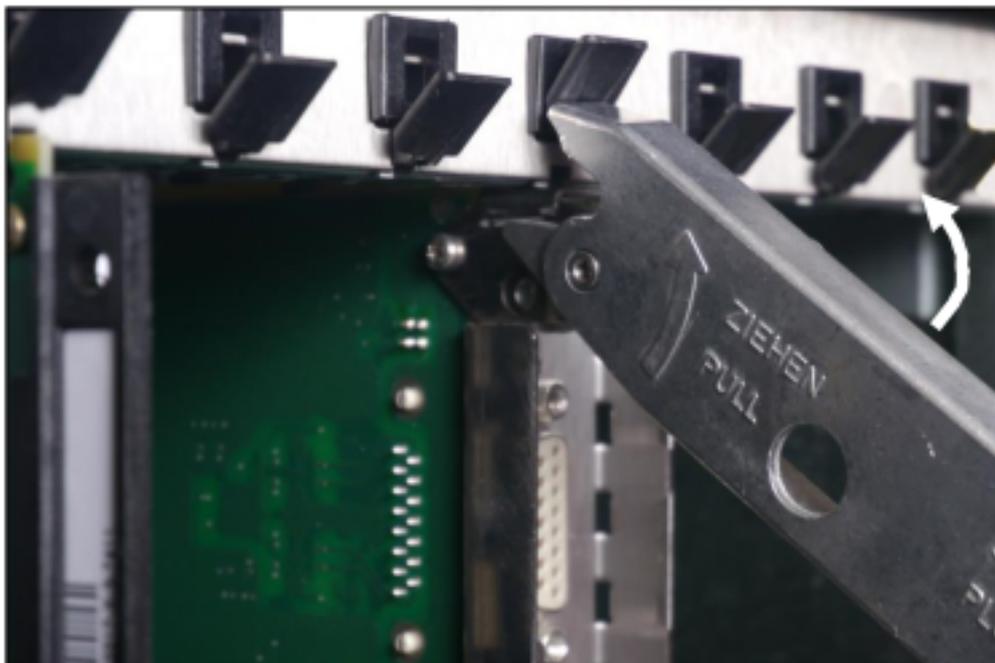
Anmerkung: Tragen Sie beim Umgang mit Baugruppen immer ein antistatisches Armband.

Die ESD-Maßnahmen zum Schutz elektrostatisch empfindlicher Geräte sind zu beachten und zu befolgen (siehe [Warnhinweise: Hinweis](#) auf Seite 16)

Schritt für Schritt

- 1) Stecken Sie die mit "Ziehen / Pull" gekennzeichnete Spitze des Baugruppenschlüssels in die obere Aussparung der Frontblende der zu entfernenden Baugruppe.

- 2) Hebeln Sie die Baugruppe aus dem Baugruppenrahmen der Systembox, indem Sie den Baugruppenschlüssel nach oben drücken.



- 3) Ziehen Sie die Baugruppe über die Führungsschienen aus der Systembox.

7.4.8.3 So installieren Sie Abschirmkappen

Durch die Installation einer Abschirmkappe können Sie sicherstellen, dass nicht verwendete Baugruppensteckplätze oder Steckplätze, die mit Peripheriebaugruppen ausgestattet sind und nur über Kunststoffblenden verfügen, ausreichend abgeschirmt sind. Folgende Baugruppen sind betroffen: STMD3, TMDID, TMEW2, SLMU, SLMAV8N, SLMAV24N.

Voraussetzungen

Die vorderen und hinteren Kunststoffblenden sind nicht an der Systembox befestigt.

Schritt für Schritt

- 1) Setzen Sie die beiden unteren Stifte der Abschirmkappen in die vorgesehenen Öffnungen auf dem Rahmen ein.

Hardwareinstallation von OpenScape Business X8

Backplanes der Systemboxen

- 2) Drücken Sie die Abschirmkappe in Richtung des Baugruppenrahmens, bis sie einrastet.



7.5 Backplanes der Systemboxen

Die Backplanes stellen die Verbindung zwischen der zentralen Steuerung OCCL, den Peripheriebaugruppen und den Stromversorgungen LUNA2 her und stellen Anschlussmöglichkeiten für Telefone, Amtsleitungen usw. zur Verfügung.

7.5.1 Backplane der Basisbox

Die Backplane der Basisbox bietet Anschlüsse für die zentrale Steuerbaugruppe OCCLA, die Peripheriebaugruppen und die Netzteile LUNA2 sowie für Telefone, Amtsleitungen usw.

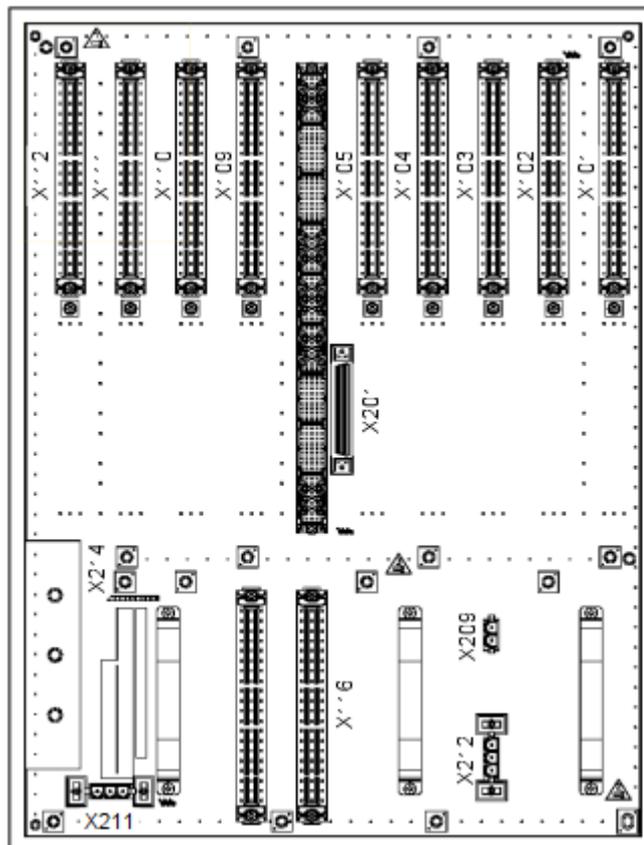


Abbildung 21: OpenScape Business X8 – Backplane der Basisbox

Tabelle 3: OpenScape Business X8 – Anschlüsse an der Backplane der Basisbox

Verbindung	Funktion
X101 bis X105, X109 bis X112	<p>SIVAPAC-Anschlüsse für die Aufnahme von Signalen von den Peripheriebaugruppen in den Steckplätzen 1 bis 5 und 9 bis 12</p> <p>Ein externer Hauptverteiler oder Patch-Panels werden über CABLUs (Cabling Units = werkseitig vorgefertigte Verkabelungseinheiten) oder Open-End-Kabel angeschlossen. Der Anschluss des S₀-Patch-Panels erfolgt über ein Open-End-Kabel.</p> <p>Die folgenden Anschluss-Panels können in die SIVAPAC-Anschlüsse eingesteckt werden:</p> <ul style="list-style-type: none"> • Anschluss-Panel mit CHAMP-Buchse zum Anschluss eines externen Hauptverteilers oder eines externen Patch-Panels über CABLUs. • Anschluss-Panels mit 8 und 24 RJ45-Buchsen zum direkten Anschluss von Telefonen, Amtsleitungen usw.

Verbindung	Funktion
X116	SIVAPAC-Anschlüsse für die Aufnahme von Signalen der Baugruppe REALS Ein externer Hauptverteiler oder Patch-Panels werden über ein Open-End-Kabel (24 DA) angeschlossen: <ul style="list-style-type: none"> • S30267-Z196-A100: 10 m Länge • S30267-Z196-A250: 25 m Länge
X201	68-polige DB68-Buchse zum Anschluss des Kabels an die Erweiterungsbox (d. h. an die DBSAP-Baugruppe)
X209	DC-Port
X211, X212	AC Stromversorgung

7.5.2 Backplane Erweiterungsbox

Die Backplane der Erweiterungsbox bietet Anschlüsse für Peripheriebaugruppen und die Netzteile LUNA2 sowie für Telefone, Amtsleitungen usw.

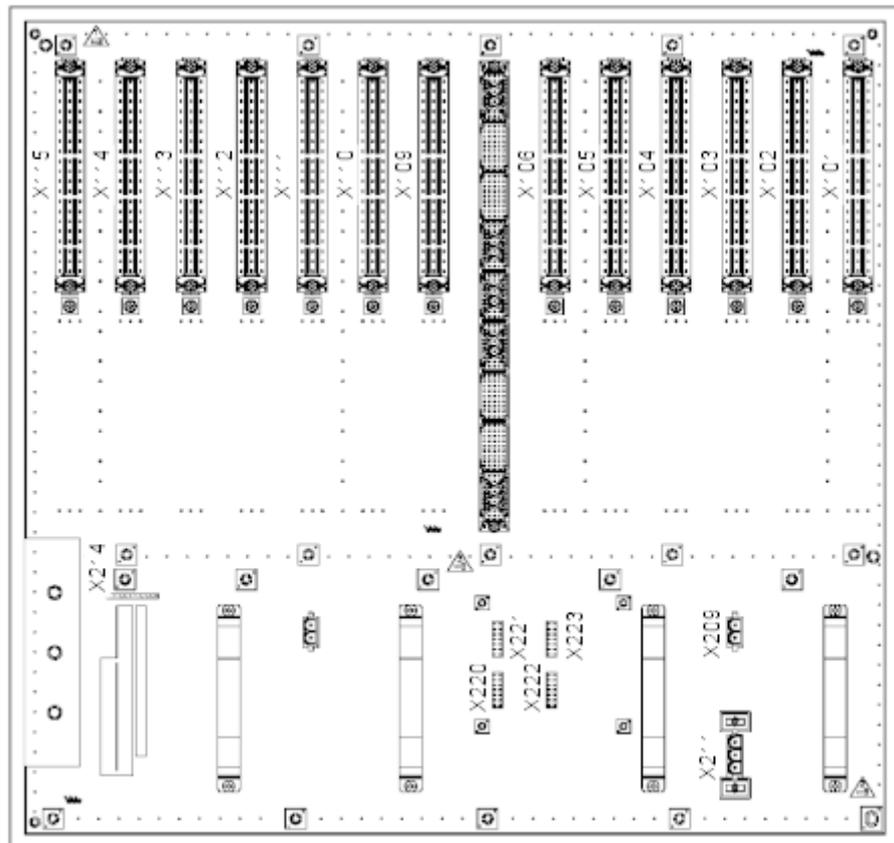


Abbildung 22: OpenScape Business X8 – Backplane Erweiterungsbox

Tabelle 4: OpenScape Business X8 – Anschlüsse an der Backplane der Erweiterungsbox

Verbindung	Funktion
X101 bis X106, X109 bis X115	<p>SIVAPAC-Anschlüsse für die Aufnahme von Signalen von den Peripheriebaugruppen in den Steckplätzen 1 bis 6 und 9 bis 15</p> <p>Ein externer Hauptverteiler oder Patch-Panels werden über CABLUs (Cabling Units = werkseitig vorgefertigte Verkabelungseinheiten) oder Open-End-Kabel angeschlossen. Der Anschluss des S₀-Patch-Panels erfolgt über ein Open-End-Kabel.</p> <p>Die folgenden Anschluss-Panels können in die SIVAPAC-Anschlüsse eingesteckt werden:</p> <ul style="list-style-type: none"> • Anschluss-Panel mit CHAMP-Buchse zum Anschluss eines externen Hauptverters oder eines externen Patch-Panels über CABLUs. • Anschluss-Panels mit 8 und 24 RJ45-Buchsen zum direkten Anschluss von Telefonen, Amtsleitungen usw.
X209	DC-Port
X211	AC Stromversorgung
X220 bis X223	<p>Anschlüsse zum Einstecken der DBSAP-Baugruppe</p> <p>DBSAP verfügt über eine 68-polige DB-68-Buchse zum Anschluss des Verbindungskabels an die Basisbox (X201).</p>

7.5.3 Anschluss- und Abschirm-Panels für Backplanes

Auf die SIVAPAC-Stecker der Backplanes der Basis- und Erweiterungsbox können Anschluss-Panels mit CHAMP-Buchse (zum Anschluss des Hauptverters MDFU-E oder eines Patch-Panels über CABLUs) und Anschluss-Panels mit RJ45-Buchsen (zum direkten Anschluss von Telefonen, Amtsleitungen usw.) gesteckt werden. Die Montage von Abschirm-Panels gewährleistet eine ausreichende Abschirmung der Backplane bei Baugruppen, deren Signale nicht über Anschluss-Panels abgegriffen werden.

Anschluss-Panel mit CHAMP-Buchse (NPPSC, S30807-Q6626-X)



Anschluss-Panel mit 24 RJ45-Buchsen (NPPAB, S30807-Q6622-X)

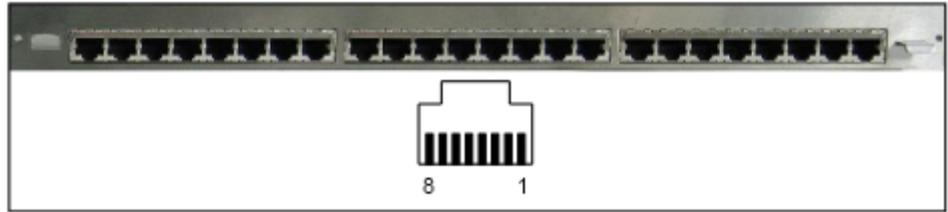


Tabelle 5: Anschluss-Panel mit 24 RJ45-Buchsen – Belegung der RJ45-Buchsen

Pin	Signal
4	a
5	b

Die RJ45-Buchsen sind zweiadrig belegt.

Anschluss-Panel mit 8 RJ45-Buchsen (NPPS0, S30807-Q6624-X)

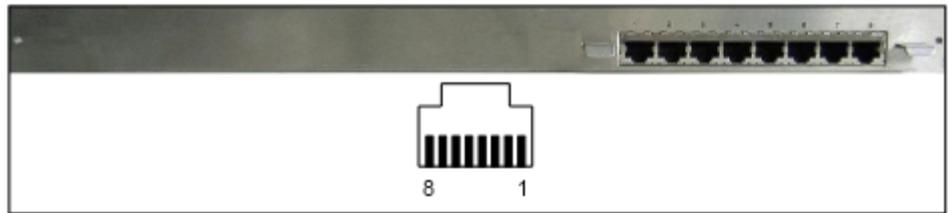


Tabelle 6: Anschluss-Panel mit 8 RJ45-Buchsen – Belegung der RJ45-Buchsen

Pin	Signal	
	Amtsanschluss/ Vernetzung	Teilnehmeranschluss
3	Senden +	Empfangen +
4	Empfangen +	Senden +
5	Empfangen –	Senden –
6	Senden –	Empfangen –

Die RJ45-Buchsen sind vieradrig belegt.

Abschirm-Panel (C39165-A7075-C44)



7.5.3.1 Wie Sie Anschluss- oder Abschirm-Panels montieren

Voraussetzungen

Die hintere Kunststoffabdeckung der Systembox ist nicht montiert.

Schritt für Schritt

Wählen Sie eine der folgenden Möglichkeiten:

- Wenn Sie ein Anschluss-Panel montieren möchten, drücken Sie dieses auf den gewünschten SIVAPAC-Stecker der Backplane.

Befestigen Sie das Anschluss-Panel mit den beiden zum Lieferumfang gehörenden Schrauben an der Systembox.

- Wenn Sie ein Abschirm-Panel montieren möchten, führen Sie eventuell vorhandene CABLUs durch die Kabeldurchführungen.

Befestigen Sie das Abschirm-Panel mit den beiden zum Lieferumfang gehörenden Schrauben an der Systembox.

7.5.4 Anschluss an Backplanes

Die Backplanes der Basis- und Erweiterungsbox stellen Anschlussmöglichkeiten für Telefone, Amtsleitungen usw. zur Verfügung. Der Anschluss kann über einen externen Hauptverteiler oder über externe Patch-Panels erfolgen. Der direkte Anschluss an die Backplane ist über Anschluss-Panels mit RJ45-Buchsen möglich.

7.5.4.1 So schließen Sie das Verbindungskabel zwischen Basis- und Erweiterungsbox an (optional)

Das Verbindungskabel (C39195-Z7611-A10) sorgt dafür, dass die Erweiterungsbox die HDLC-, PCM- und Taktsignale von der Basisbox empfängt.

Voraussetzungen

Die hinteren Kunststoffblenden der Systembox sind nicht angebracht.

Die DBSAP-Baugruppe (S30807-Q6722-X) ist auf der Backplane der Erweiterungsbox installiert.

Schritt für Schritt

- 1) Stecken Sie einen der Kabelstecker in die 68-polige DB68-Buchse X201 der Basisbox.
- 2) Stecken Sie den anderen Kabelstecker in die 68-polige DB68-Buchse der DBSAP-Baugruppe.
- 3) Befestigen Sie beide Enden des Verbindungskabels mit Kabelbindern an den Systemboxen.

7.5.4.2 So schließen Sie ein Verbindungskabel am externen Hauptverteiler an (optional)

Für den Anschluss der Backplane an den Hauptverteiler oder an andere externe Hauptverteiler stehen mehrere Möglichkeiten zur Verfügung. Diese richten sich danach, welche Peripheriebaugruppen welche Steckplätze belegen und welche Anschluss-Panels verwendet werden.

Voraussetzungen



Achtung: Elektrischer Schlag durch Berühren spannungsführender Leitungen

Schutzerden Sie die Systemboxen Ihres Kommunikationssystems und alle Hauptverteiler vor Anschluss der Telefone und Leitungen durch separate Schutzleiter.

Die vordere Kunststoffblende ist nicht an der Systembox befestigt.

Schritt für Schritt

- 1) Wählen Sie das entsprechende Verbindungskabel je nach verwendeten Peripheriebaugruppen und Anschluss-Panels.

Peripheriebaugruppe	Wenn	Dann
	Anschluss-Panel	Verbindungskabel
STMD3 TMANI TMDID TMEW2 SLMAV8N	–	Anschluss an den MDFU-E oder an einen anderen externen Hauptverteiler: Open-End-Kabel (24 DA) mit SIVAPAC-Buchse (Backplane): <ul style="list-style-type: none"> • S30267-Z196-A100: 10 m Länge • S30267-Z196-A250: 25 m Länge
	Steckerleiste mit CHAMP-Buchse	Anschluss an externen Hauptverteiler: Kabel mit CHAMP-Anschluss
SLMU SLMAV24N	–	Anschluss an externen Hauptverteiler: Open-End-Kabel (24 DA) mit SIVAPAC-Buchse (Backplane): <ul style="list-style-type: none"> • S30267-Z196-A100: 10 m Länge • S30267-Z196-A250: 25 m Länge
	Steckerleiste mit CHAMP-Buchse	Anschluss an externen Hauptverteiler: Kabel mit CHAMP-Anschluss

- 2) Stecken Sie das Verbindungskabel in den gewünschten Backplane-Anschluss.
- 3) Befestigen Sie das Kabel mit Kabelbindern an der Systembox.

- 4) Wählen Sie eine der folgenden Optionen zum Anschluss an einen externen Hauptverteiler:
 - Schließen Sie bei Verwendung eines externen Hauptverteilers und eines Open-End-Kabels das Kabel an die gewünschte Trenn-/Rangierleiste im externen Hauptverteiler an.
 - Setzen Sie bei Verwendung eines externen Hauptverteilers mit CHAMP-Anschlüssen den Stecker in die gewünschte CHAMP-Buchse des externen Hauptverteilers ein.
- 5) Befestigen Sie das Verbindungskabel mit Kabelbindern am externen Hauptverteiler.

7.5.4.3 Wie Sie die Verbindungskabel zum Patch-Panel anschließen (optional)

Für die Verbindung der Backplane mit dem Patch-Panel stehen CABLUs (24 DA) mit SIVAPAC-Steckern in den Längen 2 m (S30267-Z333-A20) und 5 m (S30267-Z333-A50) zur Verfügung.

Voraussetzungen



Achtung: Elektrischer Schlag durch Berühren spannungsführender Leitungen

Schutzerden Sie die Systemboxen Ihres Kommunikationssystems und alle Patch-Panels vor Anschluss der Telefone und Leitungen durch separate Schutzleiter.

Die hintere Kunststoffabdeckung der gewünschten Systembox ist nicht montiert.

Schritt für Schritt

- 1) Stecken Sie das Verbindungskabel auf den gewünschten Backplane-Anschluss.
- 2) Befestigen Sie das Verbindungskabel mittels Kabelbinder an der Systembox.
- 3) Stecken Sie das Verbindungskabel auf den gewünschten Anschluss des Patch-Panels.

Informationen zur Belegung der RJ45-Buchsen des Patch-Panels S30807-K6143-X siehe [Patch-Panel \(optional\)](#) auf Seite 109.

- 4) Befestigen Sie das Verbindungskabel mittels Kabelbinder am Patch-Panel.

7.5.4.4 Wie Sie die Verbindungskabel zum S₀-Patch-Panel anschließen (optional)

Für die Verbindung der Backplane (SIVAPAC-Stecker) mit dem S₀-Patch-Panel stehen Open-End-Kabel (24 DA) in den Längen 10 m (S30267-Z196-A100) und 25 m (S30267-Z196-A250) zur Verfügung.

Voraussetzungen



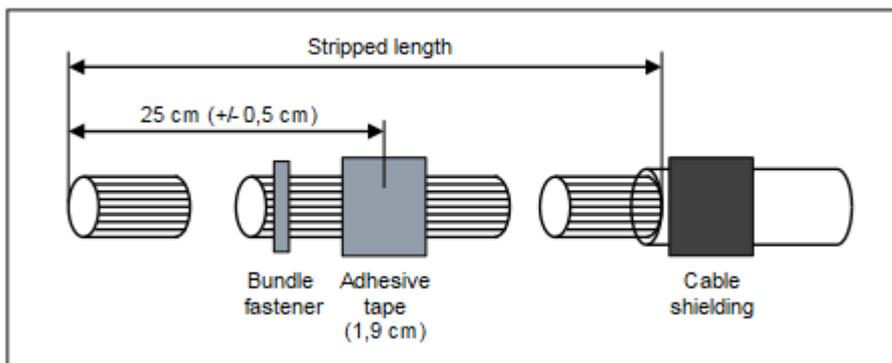
Achtung: Elektrischer Schlag durch Berühren spannungsführender Leitungen

Schutzerden Sie die Systemboxen Ihres Kommunikationssystems vor Anschluss der Telefone und Leitungen durch separate Schutzleiter.

Die hintere Kunststoffabdeckung der gewünschten Systembox ist nicht montiert.

Schritt für Schritt

- 1) Stecken Sie das Verbindungskabel auf den gewünschten Backplane-Anschluss.
- 2) Befestigen Sie das Verbindungskabel mittels Kabelbinder an der Systembox.
- 3) Legen Sie die Adern des Kabels frei (Abmantellänge = 60 cm (+/- 0,5 cm)).



- 4) Legen Sie den Kabelschirm des Kabels auf einer Länge von ca. 3 cm frei. Kürzen Sie den Beidraht auf ca. 2,5 cm und fixieren Sie diesen auf dem Kabelschirm, indem Sie diesen mit Klebeband umwickeln (mindestens 1,5fache Umwicklung).
- 5) Legen Sie Kabeladern mit einem Standard-Auflegewerkzeug am S₀-Patch-Panel auf. Die Kabeladern sind vor dem Auflegen zu verdrehen (siehe folgendes Bild).

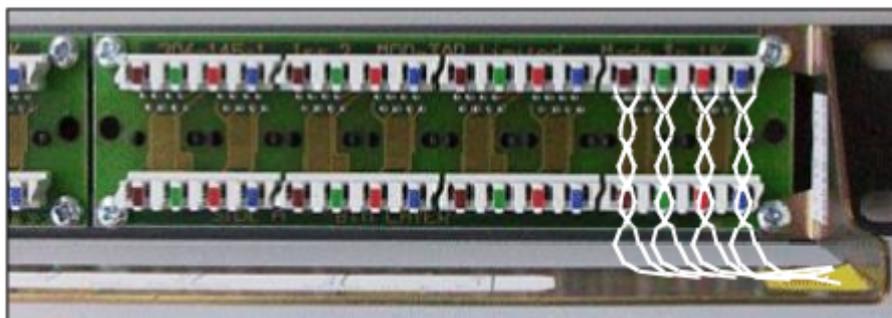


Tabelle 7: Farbcode für Open-End-Kabel

Farbgruppe	Paar	a-Ader	b-Ader
1	1	weiß/blau	blau/weiß
		weiß/orange	orange/weiß
	2	weiß/grün	grün/weiß
	3		

Farbgruppe	Paar	a-Ader	b-Ader
	4	weiß/braun	
			braun/weiß
	5	weiß/grau	
			grau/weiß
2	6	rot/blau	
			blau/rot
	7	rot/orange	
			orange/rot
	8	rot/grün	
			grün/rot
	9	rot/braun	
			braun/rot
10	rot/grau		
		grau/rot	
3	11	schwarz/blau	
			blau/schwarz
	12	schwarz/orange	
			orange/schwarz
	13	schwarz/grün	
			grün/schwarz
	14	schwarz/braun	
			braun/schwarz
15	schwarz/grau		
		grau/schwarz	
4	16	gelb/blau	
			blau/gelb
	17	gelb/orange	
			orange/gelb
	18	gelb/grün	
			grün/gelb
	19	gelb/braun	
			braun/gelb
20	gelb/grau		
		grau/gelb	
5	21	violett/blau	
			blau/violett

Farbgruppe	Paar	a-Ader	b-Ader
	22	violett/orange	
			orange/violett
	23	violett/grün	
			grün/violett
	24	violett/braun	
			braun/violett

Informationen zur Belegung der RJ45-Buchsen des S₀-Patch-Panels C39104-Z7001-B3 für den Teilnehmeranschluss und für den Amtsanschluss siehe [Patch-Panels \(optional\)](#).

- 6) Befestigen Sie das Verbindungskabel mittels Kabelbinder am S₀-Patch-Panel.

7.6 Amtsanschluss

Das OpenScape Business X8 Kommunikationssystem bietet verschiedene Möglichkeiten für Amtsanschlüsse und damit für den Zugang zum öffentlichen Kommunikationsnetz.

Sie können den oder die erforderlichen Amtsanschlüsse für Ihr Kommunikationssystem aus den folgenden Optionen wählen:

- ISDN-Anlagenanschluss oder ISDN-Mehrgeräteanschluss über eine S₀-Schnittstelle (nicht für USA und Kanada)
- ISDN-Primärmultiplexanschluss über eine S_{2M}-Schnittstelle (nicht für USA und Kanada)
- ISDN-Primärmultiplexanschluss über die T1-Schnittstelle (nicht für USA und Kanada)
- Amtsanschluss mit CAS-Protokoll über CAS-Schnittstelle (nur für ausgewählte Länder)
- Analoge Amtsanschlüsse

7.6.1 So richten Sie einen ISDN-Anlagenanschluss oder ISDN-Mehrgeräteanschluss über einen S₀-Port ein (nicht für USA und Kanada)

Voraussetzungen



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

Schutzerden Sie die Systemboxen Ihres Kommunikationssystems und alle Hauptverteiler und Patch-Panels vor Anschluss der Telefone und Leitungen durch separate Schutzleiter.

Eine Schutzerdung des S₀-Patch-Panels (C39104-Z7001-B3) ist nicht erforderlich.



ACHTUNG: Brandgefahr

Um das Brandrisiko zu verringern, dürfen Sie nur Kommunikationsleitungen mit einem Leiterdurchmesser von mindestens 0,4 mm (AWG 26) oder größer verwenden.

OpenScape Business X8 ist mit mindestens einer Baugruppe STMD3 ausgestattet.

Beim Startvorgang muss die S₀-Schnittstelle als ISDN-Anlagenanschluss oder ISDN-Mehrgeräteanschluss konfiguriert werden.

Ein ISDN-Anlagenanschluss oder ISDN-Mehrgeräteanschluss ist verfügbar.

Schritt für Schritt

Verbinden Sie den gewünschten S₀-Port mit dem NTBA des ISDN-Anlagenanschlusses oder ISDN-Mehrgeräteanschlusses.

Wählen Sie dazu eine der folgenden Möglichkeiten:

- Wenn die Verbindung über den externen Hauptverteiler MDFU erfolgt, schließen Sie das NTBA-Verbindungskabel an die gewünschte Trennleiste/Rangierleiste des MDFU-E an.
- Wenn die Verbindung über das externe S₀-Patch-Panel erfolgt, schließen Sie das NTBA-Verbindungskabel an die gewünschte RJ45-Buchse des S₀-Patch-Panels an.
- Wenn die Verbindung über die Backplane einer Systembox erfolgt (d. h. über ein Anschluss-Panel mit acht RJ45-Buchsen), schließen Sie das NTBA-Verbindungskabel an die gewünschte RJ45-Buchse des gewünschten Anschluss-Panels an.

7.6.2 So richten Sie einen ISDN-Primärmultiplexanschluss über einen S_{2M}-Port ein (nicht für USA und Kanada)

Voraussetzungen



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

Schutzerden Sie die Systemboxen Ihres Kommunikationssystems und alle Hauptverteiler und Patch-Panels vor Anschluss der Telefone und Leitungen durch separate Schutzleiter.



ACHTUNG: Brandgefahr

Um das Brandrisiko zu verringern, dürfen Sie nur Kommunikationsleitungen mit einem Leiterdurchmesser von mindestens 0,4 mm (AWG 26) oder größer verwenden.

OpenScape Business X8 ist mit mindestens einer Baugruppe DIUT2 ausgestattet.

Ein ISDN-Primärmultiplexanschluss ist verfügbar.

Schritt für Schritt

Verbinden Sie den gewünschten Sub-D-Stecker an der Vorderseite der gewünschten Baugruppe mit dem NTPM des ISDN-Primärmultiplexanschlusses.

7.6.3 So richten Sie einen ISDN-Primärmultiplexanschluss über eine T1-Schnittstelle ein (nur für USA und Kanada)

Voraussetzungen



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

Schutzerden Sie die Systemboxen Ihres Kommunikationssystems und alle Hauptverteiler und Patch-Panels vor Anschluss der Telefone und Leitungen durch separate Schutzleiter.



ACHTUNG: Brandgefahr

Um das Brandrisiko zu verringern, dürfen Sie nur Kommunikationsleitungen mit einem Leiterdurchmesser von mindestens 0,4 mm (AWG 26) oder größer verwenden.

OpenScape Business X8 ist mit mindestens einer Baugruppe DIUT2 ausgestattet.

Eine Channel Service Unit (CSU), die nach FCC Part 68 zugelassen ist und die ANSI-Vorschrift T1.403 erfüllt, ist verfügbar. Die T1-Schnittstelle darf nicht direkt mit dem PSTN (Public Switched Telephone Network) verbunden werden. Es ist wichtig, dass eine CSU zwischen dem Kommunikationssystem und dem digitalen Amtsanschluss installiert wird. Durch die CSU erhält OpenScape BusinessX8 folgende Merkmale: Isolierung und Überspannungsschutz des Kommunikationssystems, Diagnosemöglichkeiten im Fehlerfall (zum Beispiel Signal Loop Back, Einfügen von Testsignalen und Testmustern), Einpegeln des Ausgangssignals entsprechend den vom Netzanbieter vorgeschriebenen Leitungslängen. Eine CSU ist nicht im Lieferumfang des OpenScape Business X8 Kommunikationssystems enthalten.

Ein ISDN-Primärmultiplexanschluss ist verfügbar.

Schritt für Schritt

Verbinden Sie den gewünschten Sub-D-Stecker an der Vorderseite der gewünschten Baugruppe mit der Channel Service Unit (CSU) an.

7.6.4 Nur für ausgewählte Länder: Wie Sie einen Amtsanschluss über eine E1-CAS-Schnittstelle durchführen

Voraussetzungen

**Achtung:**

Elektrischer Schlag durch Berühren spannungsführender Leitungen

Schutzerden Sie die Systemboxen Ihres Kommunikationssystems und alle Hauptverteiler und Patch-Panels vor Anschluss der Telefone und Leitungen durch separate Schutzleiter.

**ACHTUNG:** Brandgefahr

Um das Brandrisiko zu verringern, dürfen Sie nur Kommunikationsleitungen mit einem Leiterdurchmesser von mindestens 0,4 mm (AWG 26) oder größer verwenden.

OpenScape Business X8 ist mit mindestens einer Baugruppe TMCAS2 oder TMCAS bestückt.

Ein Amtsanschluss mit CAS-Protokoll steht zur Verfügung.

Schritt für Schritt

Verbinden Sie die gewünschte CAS-Schnittstelle in der Frontblende der gewünschten Baugruppe mit dem NT des Amtsanschlusses.

7.6.5 So richten Sie eine analoge Amtsleitung ein

Voraussetzungen

**Achtung:**

Elektrischer Schlag durch Berühren spannungsführender Leitungen

Schutzerden Sie die Systemboxen Ihres Kommunikationssystems und alle Hauptverteiler und Patch-Panels vor Anschluss der Telefone und Leitungen durch separate Schutzleiter.

**ACHTUNG:** Brandgefahr

Um das Brandrisiko zu verringern, dürfen Sie nur Kommunikationsleitungen mit einem Leiterdurchmesser von mindestens 0,4 mm (AWG 26) oder größer verwenden.

Anmerkung:

Brandgefahr durch Überspannung

Hardwareinstallation von OpenScape Business X8

Anschluss von Telefonen und Geräten

Bei Leitungslängen über 500 m und bei Leitungen, die das Gebäude verlassen, müssen die Baugruppen TMANI und TMDID durch einen externen Blitzschutz geschützt werden.

Ein solcher Blitzschutz wird als zusätzlicher Primärschutz bezeichnet. Der zusätzliche Primärschutz wird durch den 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.

OpenScape Business X8 ist mit mindestens einem Baugruppe TMANI oder TMDID ausgestattet.

Nur für USA und Kanada: Ein Sicherungselement gemäß UL 497A oder CSA C22.2 Nr. 226 ist erhältlich. Aufgrund der Installationsvorschriften muss der Anschluss von analogen Amtsleitungen über genehmigte Sicherungselemente gemäß UL 497A oder CSA C22.2 Nr.226 erfolgen.

Eine analoge Amtsleitung HKZ-Signalverfahren (Ground Start oder Loop Start) ist verfügbar.

Schritt für Schritt

Schließen Sie den gewünschten Port a/b der gewünschten Baugruppe an die TAE-Buchse des analogen Amtsanschlusses an.

Wählen Sie dazu eine der folgenden Möglichkeiten:

- Wenn die Verbindung über den externen Hauptverteiler MDFU erfolgt, schließen Sie das TAE-Verbindungskabel an die gewünschte Trennleiste/Rangierleiste des MDFU an.
- Wenn die Verbindung über das externe-Patch-Panel erfolgt, schließen Sie das TAE-Verbindungskabel an die gewünschte RJ45-Buchse des-Patch-Panels an.
- Wenn die Verbindung über die Backplane einer Systembox erfolgt (d. h. über ein Anschluss-Panel mit 24 RJ45-Buchsen), schließen Sie das TAE-Verbindungskabel an die gewünschte RJ45-Buchse des gewünschten Anschluss-Panels an.

7.7 Anschluss von Telefonen und Geräten

Das Kommunikationssystem OpenScape Business X8 bietet verschiedene Möglichkeiten zum Anschluss von Telefonen und Geräten.

Sie können den oder die erforderlichen Anschlüsse für Ihr Kommunikationssystem aus den folgenden Optionen wählen:

- Direkter Anschluss von ISDN-Telefonen (nicht für USA und Kanada)
- Anschluss von ISDN-Telefonen über den S₀-Bus (nicht für USA und Kanada)
- Anschluss von U_{P0/E}-Telefonen
- Anschluss von analogen Telefonen und Geräten

Anmerkung: An eine a/b-Schnittstelle kann nur ein analoges Gerät angeschlossen werden.

7.7.1 So schließen Sie ISDN-Telefone direkt an (nicht für USA und Kanada)

Voraussetzungen



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

Schutzerden Sie die Systemboxen Ihres Kommunikationssystems und alle Hauptverteiler und Patch-Panels vor Anschluss der Telefone und Leitungen durch separate Schutzleiter.

Eine Schutzerdung des S₀-Patch-Panels (C39104-Z7001-B3) ist nicht erforderlich.



ACHTUNG:

Brandgefahr

Um das Brandrisiko zu verringern, dürfen Sie nur Kommunikationsleitungen mit einem Leiterdurchmesser von mindestens 0,4 mm (AWG 26) oder größer verwenden.

Anmerkung:

Brandgefahr durch Überspannung

Nur für die Schnittstellen für den Teilnehmeranschluss: Bei Leitungslängen über 500 m und bei Leitungen, die das Gebäude verlassen, muss die Baugruppe STMD3 durch einen externen Blitzschutz geschützt werden.

Ein solcher Blitzschutz wird als zusätzlicher Primärschutz bezeichnet. Der zusätzliche Primärschutz wird durch den 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.

OpenScape Business X8 ist mit mindestens einer Baugruppe STMD3 ausgestattet.

Die verwendeten S₀-Ports müssen beim Start als interner S₀-Anschluss konfiguriert werden.

Die anzuschließenden ISDN-Telefone müssen über eine eigene Speisung verfügen, zum Beispiel über ein Steckernetzgerät. Es ist nicht möglich, Strom über die S₀-Ports der Baugruppe STMD3 zu beziehen.

Schritt für Schritt

1) Verbinden Sie den gewünschten S₀-Port mit dem ISDN-Telefon.

Wählen Sie dazu eine der folgenden Möglichkeiten:

- Wenn die Verbindung über den externen Hauptverteiler MDFU-E erfolgt, schließen Sie das Verbindungskabel des ISDN-Telefons an die gewünschte Trennleiste des MDFU-E an.
- Wenn die Verbindung über das externe S₀-Patch-Panel erfolgt, schließen Sie das Verbindungskabel des ISDN-Telefons an die gewünschte RJ45-Buchse des S₀-Patch-Panels an.
- Wenn die Verbindung über die Backplane einer Systembox erfolgt (d. h. über ein Anschluss-Panel mit acht RJ45-Buchsen), schließen Sie das Verbindungskabel des ISDN-Telefons an die gewünschte RJ45-Buchse des gewünschten Anschluss-Panels an.

Tipp: Beachten Sie die Installationsanweisungen des anzuschließenden Telefons.

2) Falls vorhanden, schließen Sie weitere ISDN-Telefone mit der gleichen Methode an das Kommunikationssystem an.

7.7.2 So schließen Sie ISDN-Telefone über den S₀-Bus an (nicht für USA und Kanada)

Voraussetzungen



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

Schutzerden Sie die Systemboxen Ihres Kommunikationssystems und alle Hauptverteiler und Patch-Panels vor Anschluss der Telefone und Leitungen durch separate Schutzleiter.

Eine Schutzerdung des S₀-Patch-Panels (C39104-Z7001-B3) ist nicht erforderlich.



ACHTUNG:

Brandgefahr

Um das Brandrisiko zu verringern, dürfen Sie nur Kommunikationsleitungen mit einem Leiterdurchmesser von mindestens 0,4 mm (AWG 26) oder größer verwenden.

Anmerkung:

Brandgefahr durch Überspannung

Nur für die Schnittstellen für den Teilnehmeranschluss: Bei Leitungslängen über 500 m und bei Leitungen, die das Gebäude

verlassen, muss die Baugruppe STMD3 durch einen externen Blitzschutz geschützt werden.

Ein solcher Blitzschutz wird als zusätzlicher Primärschutz bezeichnet. Der zusätzliche Primärschutz wird durch den 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.

OpenScape Business X8 ist mit mindestens einer Baugruppe STMD3 ausgestattet.

Die verwendeten S₀-Ports müssen beim Start als interner S₀-Anschluss konfiguriert werden.

Die anzuschließenden ISDN-Telefone müssen über eine eigene Speisung verfügen, zum Beispiel über ein Steckernetzgerät. Es ist nicht möglich, Strom über die S₀-Ports der Baugruppe STMD3 zu beziehen.

Jedem einzelnen ISDN-Telefon (ISDN-Teilnehmer) muss eine eindeutige Mehrfachrufnummer (MSN = Multiple Subscriber Number) zugeordnet werden. Diese Zuordnung ist im Konfigurationsmenü des ISDN-Teilnehmers durchzuführen.

Schritt für Schritt

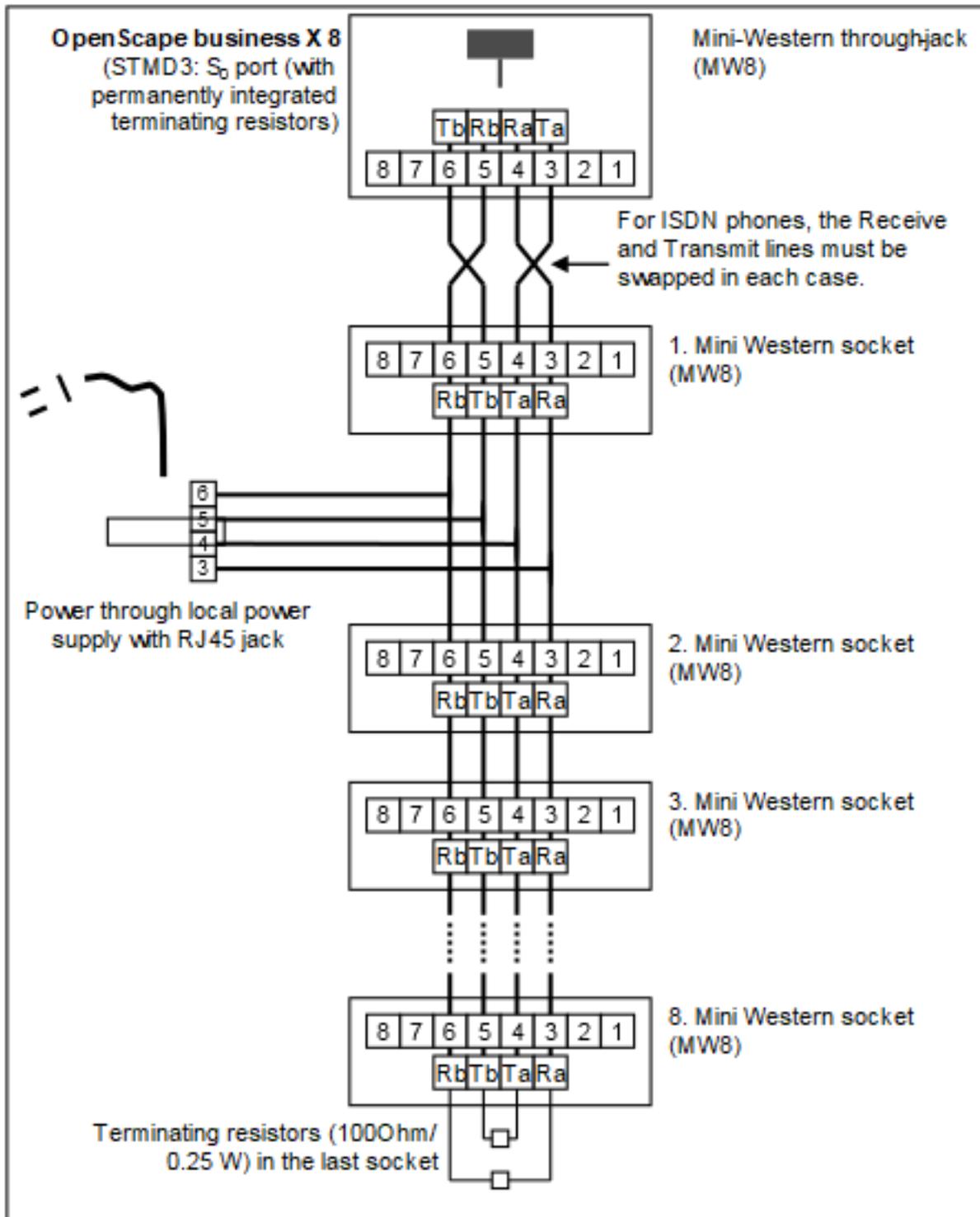
1) Verbinden Sie den gewünschten S₀-Port mit der Mini-Western-Buchse auf dem S₀-Bus.

Wählen Sie dazu eine der folgenden Möglichkeiten:

- Wenn die Verbindung über den externen Hauptverteiler MDFU erfolgt, schließen Sie das Verbindungskabel der Mini-Western-Buchse auf dem S₀-Bus an die gewünschte Trennleiste des MDFU an.
- Wenn die Verbindung über das externe S₀-Patch-Panel erfolgt, schließen Sie das Verbindungskabel der Mini-Western-Buchse auf dem S₀-Bus an die gewünschte RJ45-Buchse des Patch-Panels an.
- Wenn die Verbindung über die Backplane einer Systembox erfolgt (d. h. über ein Anschluss-Panel mit acht RJ45-Buchsen), schließen Sie das Verbindungskabel der Mini-Western-Buchse auf dem S₀-Bus an die gewünschte RJ45-Buchse des gewünschten Anschluss-Panels an.

Hardwareinstallation von OpenScape Business X8

2) Schließen Sie die Verdrahtung wie in der folgenden Abbildung gezeigt ab.



3) Installieren Sie die Abschlusswiderstände (100 Ohm/0,25 W) auf der letzten Buchse im S₀-Bus.

- 4) Achten Sie darauf, dass die Abschlusswiderstände nur an den beiden Enden des S₀-Bus angeschlossen sind. Für die anderen Buchsen auf dem S₀-Bus sind keine Abschlusswiderstände erforderlich.

Tipp: Da Abschlusswiderstände bereits in OpenScape Business X8 integriert sind, bildet das Kommunikationssystem ein Ende eines S₀-Bus.

Tipp: Beachten Sie die Installationsanweisungen des anzuschließenden Telefons.

7.7.3 So schließen Sie U_{P0/E}-Telefone an

Voraussetzungen



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

Schutzerden Sie die Systemboxen Ihres Kommunikationssystems und alle Hauptverteiler und Patch-Panels vor Anschluss der Telefone und Leitungen durch separate Schutzleiter.



ACHTUNG:

Brandgefahr

Um das Brandrisiko zu verringern, dürfen Sie nur Kommunikationsleitungen mit einem Leiterdurchmesser von mindestens 0,4 mm (AWG 26) oder größer verwenden.

Anmerkung:

Brandgefahr durch Überspannung

Bei Leitungslängen über 500 m und bei Leitungen, die das Gebäude verlassen, müssen die Baugruppen SLMO2 und SLMO8 durch einen externen Blitzschutz geschützt werden.

Ein solcher Blitzschutz wird als zusätzlicher Primärschutz bezeichnet. Der zusätzliche Primärschutz wird durch den 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.

OpenScape Business X8 ist mit mindestens einer SLMU-Baugruppe ausgestattet.

Schritt für Schritt

- 1) Verbinden Sie den gewünschten U_{P0/E}-Anschluss mit dem U_{P0/E}-Telefon.

Wählen Sie dazu eine der folgenden Möglichkeiten:

- Wenn die Verbindung über den externen Hauptverteiler MDFU erfolgt, schließen Sie das Verbindungskabel des U_{P0/E}-Telefons an die gewünschte Trennleiste/Rangierleiste des MDFU an.
- Wenn die Verbindung über das externe Patch-Panel erfolgt, schließen Sie das Verbindungskabel des U_{P0/E}-Telefons an die gewünschte RJ45-Buchse des Patch-Panels an.
- Wenn die Verbindung über die Backplane einer Systembox erfolgt (d. h. über ein Anschluss-Panel mit 24 RJ45-Buchsen), schließen Sie das Verbindungskabel des U_{P0/E}-Telefons an die gewünschte RJ45-Buchse des gewünschten Anschluss-Panels an.

Tipp: Beachten Sie die Installationsanweisungen des anzuschließenden Telefons.

- 2) Falls vorhanden, schließen Sie weitere U_{P0/E}-Telefone mit der gleichen Methode an das Kommunikationssystem an.

7.7.4 So schließen Sie analoge Telefone und Geräte an

Voraussetzungen



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

Schutzerden Sie die Systemboxen Ihres Kommunikationssystems und alle Hauptverteiler und Patch-Panels vor Anschluss der Telefone und Leitungen durch separate Schutzleiter.



ACHTUNG:

Brandgefahr

Um das Brandrisiko zu verringern, dürfen Sie nur Kommunikationsleitungen mit einem Leiterdurchmesser von mindestens 0,4 mm (AWG 26) oder größer verwenden.

Anmerkung:

Brandgefahr durch Überspannung

Bei Leitungslängen über 500 m und bei Leitungen, die das Gebäude verlassen, müssen die Baugruppen SLMAV8N und SLMAV24N durch einen externen Blitzschutz geschützt werden.

Ein solcher Blitzschutz wird als zusätzlicher Primärschutz bezeichnet. Der zusätzliche Primärschutz wird durch den 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.

OpenScape Business X8 ist mit mindestens einer Bauruppe SLMAV8N oder SLMAV24N ausgestattet.

Schritt für Schritt

- 1) Schließen Sie den gewünschten Port a/b für die Verbindung mit dem analogen Gerät (Telefon, Fax, Modem, Lautsprecher usw.) an.

Wählen Sie dazu eine der folgenden Möglichkeiten:

- Wenn die Verbindung über den externen Hauptverteiler MDFU erfolgt, schließen Sie das Verbindungskabel des analogen Telefons oder Geräts an die gewünschte Trennleiste/Rangierleiste des MDFU an.
 - Wenn die Verbindung über das externe Patch-Panel erfolgt, schließen Sie das Verbindungskabel des analogen Telefons oder Geräts an die gewünschte RJ45-Buchse des Patch-Panels an.
 - Wenn die Verbindung über die Backplane einer Systembox erfolgt (d. h. über ein Anschluss-Panel mit 24 RJ45-Buchsen), schließen Sie das Verbindungskabel des analogen Telefons oder Geräts an die gewünschte RJ45-Buchse des gewünschten Anschluss-Panels an.
- 2) Falls vorhanden, schließen Sie weitere analoge Telefone oder Geräte mit der gleichen Methode an das Kommunikationssystem an.

7.8 Abschließende Tätigkeiten

Um die Installation abzuschließen, müssen M.2 SSD oder SDHC-Karte eingesetzt und eine Sichtprüfung vorgenommen werden. Außerdem müssen bei Standalone-Installationen alle Systemboxen des Kommunikationssystems mit den dafür vorgesehenen Kunststoffabdeckungen verschlossen werden. Schließlich wird das System an die Netzspannungsversorgung angeschlossen.

Das Kommunikationssystem kann dann mit dem OpenScape Business Assistant (WBM) in Betrieb genommen werden. Die Beschreibung dafür finden Sie in der Online-Hilfe des WBM oder in der Administratordokumentation im Kapitel „Erstinstallation OpenScape Business“.

Anmerkung: Bei der Erstinbetriebnahme des Kommunikationssystems ist der Ladezustand des Akkus auf dem Mainboard nicht definiert. Um einen ausreichenden Ladezustand zu erreichen, muss das System mindestens 2 Tage am Stromnetz bleiben. Wenn das System von der Netzspannungsversorgung getrennt wird, kann der Akku nicht ausreichend geladen sein und möglicherweise dazu führen, dass die Aktivierungszeit aufgrund von Zeitmanipulationen blockiert wird.

7.8.1 So setzen Sie die M.2 SSD oder die SDHC-Karte ein (System mit OCCM)

Die M.2 SSD oder die SDHC-Karte enthält die OpenScape Business Kommunikationssoftware und muss vor dem Starten des Kommunikationssystems eingebaut/eingesetzt werden.

Schritt für Schritt

- 1) Vergewissern Sie sich, dass der Schreibschutz der SDHC-Karte deaktiviert ist (Schalter Richtung Metallkontakte).
- 2) Stecken Sie die SDHC-Karte in den SDHC-Steckplatz des Mainboards, bis sie einrastet. Die Metallkontakte der SDHC-Karte müssen dabei Richtung Mainboard zeigen.

7.8.2 So nehmen Sie eine Sichtprüfung vor

Vor dem Starten des Kommunikationssystems müssen Sie eine Sichtprüfung von Hardware, Kabeln und Stromversorgung vornehmen.

Voraussetzungen



GEFAHR:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

Trennen Sie sämtliche Versorgungsstromkreise des Kommunikationssystems, bevor Sie eine Sichtprüfung vornehmen:

- Trennen Sie die Batteriespannung, die Versorgungsspannung (LUNA2) und die Netzspannung.
- Ziehen Sie die Anschlussleitungen aller eventuell angeschlossenen Akkupacks oder eventuell angeschlossenen Akkus ab.
- Ziehen Sie alle Netzanschlusstecker des Kommunikationssystems.

Anmerkung:

Tragen Sie beim Umgang mit Baugruppen immer ein antistatisches Armband.

Die ESD-Maßnahmen zum Schutz elektrostatisch empfindlicher Geräte sind zu beachten und zu befolgen (siehe [Warnhinweise: Hinweis](#)).

Die vorderen und hinteren Kunststoffabdeckungen sind nicht an den Systemboxen befestigt.

Schritt für Schritt

- 1) Trennen Sie sämtliche Versorgungsstromkreise des Kommunikationssystems.
- 2) Achten Sie darauf, dass das Kommunikationssystem spannungsfrei ist.

- 3) Achten Sie darauf, dass M.2 SSD oder SDHC-Karte richtig eingesetzt sind. Der Schreibschutz der SDHC-Karte muss deaktiviert sein (Schalter Richtung Metallkontakte).
- 4) Vergewissern Sie sich, dass alle Baugruppen sicher sind.
Überprüfen Sie ggf., ob die betroffenen Baugruppen richtig eingesetzt wurden (siehe [So setzen Sie eine Baugruppe ein](#)).
- 5) Achten Sie darauf, dass alle Verbindungskabel richtig verlegt und gesichert wurden. Besteht zum Beispiel die Gefahr, über ein Kabel zu stolpern?
Achten Sie ggf. darauf, dass die Verbindungskabel richtig installiert sind.
- 6) Vergewissern Sie sich, dass die Abschirmkappen für nicht verwendete Steckplätze oder Steckplätze, die mit Peripheriebaugruppen ausgestattet sind, die nur Kunststoffabdeckungen haben, richtig installiert sind.
Installieren Sie ggf. die fehlenden Abschirmkappen (siehe [So installieren Sie Abschirmkappen](#)).
- 7) Prüfen Sie, ob die Steckplätze für die LUNA2-Netzteile und die REALS-Baugruppe in der Basisbox von einer äußeren Platte abgedeckt sind.
Bringen Sie bei Bedarf die fehlende Außenplatte an.
- 8) Prüfen Sie, ob die Steckplätze für die LUNA2-Netzteile und die REALS-Baugruppe in der Erweiterungsbox (falls vorhanden) von einer äußeren Platte abgedeckt sind.
Bringen Sie bei Bedarf die fehlende Außenplatte an.
- 9) Prüfen Sie das Vorhandensein von Abschirmblenden auf der Backplane von Baugruppen, die keine Anschlussblenden haben.
Installieren Sie ggf. die fehlende Abschirmblende (siehe [So montieren Sie Anschluss- oder Abschirmblenden](#)).
- 10) Prüfen Sie, ob ein separater Schutzleiter an der Schutzerdungsklemme jeder Systembox angeschlossen ist.
Führen Sie bei Bedarf die separate Erdung aller Systemboxen durch (siehe [Schutzerdung für Standalone-Installationen](#) und [Schutzerdung für 19-Zoll-Rackmontagen](#)).
- 11) Achten Sie darauf, dass alle verwendeten Hauptverteiler und/oder Patch-Panels richtig mit dem Schutzleiter verbunden sind.
Führen Sie bei Bedarf die separate Erdung aller Hauptverteiler und/oder Patch-Panels durch (siehe [Schutzerdung für Standalone-Installationen](#) und [Schutzerdung für 19-Zoll-Rackmontagen](#)).
- 12) Prüfen Sie, ob die Nennspannung der Netzspannungsversorgung mit der Nennspannung des Kommunikationssystems übereinstimmt (Typenschild).

Nächste Schritte

Nur für Standalone-Installationen: Schließen sie alle Systemboxen des Kommunikationssystems mit den dafür vorgesehenen Kunststoffabdeckungen (siehe [Nur bei freistehender Montage: Wie Sie die Kunststoffabdeckungen einer Systembox montieren](#) auf Seite 156).

7.8.3 Nur bei freistehender Montage: Wie Sie die Kunststoffabdeckungen einer Systembox montieren

Bei freistehender Montage müssen alle Systemboxen vor der Inbetriebnahme des Kommunikationssystems mit den dafür vorgesehenen Kunststoffabdeckungen verschlossen werden.

Schritt für Schritt

- 1) Platzieren Sie die an der Unterkante einer Kunststoffabdeckung befindlichen Stifte in die Führungsschlitze der Vorderseite der Basisbox.
- 2) Drücken Sie die Kunststoffabdeckung bis zum Einrasten in Richtung Basisbox.



- 3) Wiederholen Sie die Schritte 1 und 2, um die Kunststoffabdeckung auf der Rückseite der Basisbox zu montieren.
- 4) Wiederholen Sie die Schritte 1 bis 3, um die Kunststoffabdeckungen einer eventuell vorhandenen Erweiterungsbox zu montieren.

7.8.4 Wie Sie das System ans Stromnetz anschließen

Schritt für Schritt

Stecken Sie das Netzanschlusskabel in die Buchse der Stromversorgung. Das Kommunikationssystem fährt hoch.

Anmerkung: Lassen Sie das System mindestens 2 Tage am Stromnetz, damit der Akku des Mainboards einen ausreichenden Ladezustand erreicht. Bei unzureichendem Ladezustand kann es vorkommen, dass bei wiederholtem Hochfahren des Systems die Activation Period wegen Zeitmanipulation gesperrt wird.

8 Installation des Linux-Servers

Für OpenScape Business S und OpenScape Business UC Booster Server wird die OpenScape Business Kommunikationssoftware auf einem Linux-Betriebssystem installiert. Die Kommunikationssoftware kann direkt auf einem Linux-Server oder in einer virtuellen Umgebung mit VMware vSphere oder Microsoft Hyper-V betrieben werden.

Anmerkung: Wenn im Folgenden sowohl OpenScape Business S als auch OpenScape Business UC Booster Server gemeint sein kann, wird zur Vereinfachung nur noch von OpenScape Business geschrieben.

Als Linux-Betriebssystem ist entweder die reguläre SLES 12 SP5 64 Bit Version zu installieren oder eine vom Server-PC-Hersteller optimierte SLES 12 SP5 64 Bit Version.

In dieser Installationsanleitung ist die Erstinbetriebnahme des Linux-Servers beschrieben. Sie ist abhängig davon, ob der Linux-Server einen Software-RAID nutzt oder nicht. Die Installation der OpenScape Business Kommunikationssoftware und die weitere Konfiguration von OpenScape Business sind in der *OpenScape Business Administratordokumentation* beschrieben.

Die Erstinbetriebnahme des Linux-Servers ist für die Oberflächensprache Englisch beschrieben. Selbstverständlich kann die Installation und Konfiguration auch in einer anderen Oberflächensprache durchgeführt werden.

8.1 Voraussetzungen

Nachfolgend sind die Voraussetzungen und Randbedingungen beschrieben, um OpenScape Business auf dem Linux-Server (Server-PC) betreiben zu können.

Hardware

Der Server-PC muss folgende Mindestvoraussetzungen erfüllen:

- 64 Bit fähig
- ausgelegt für 24h-Betrieb
- Zertifiziert vom PC-Hersteller für SLES 12 SP5 64 Bit
- die Kommunikationssoftware für OpenScape Business ist die einzige Anwendung (ausgenommen Virens Scanner)
- mind. 2-Kern-Prozessor ab 2,0 GHz pro Kern (mit OpenScape Business Contact Center oder ab 500 Benutzer: mind. 4-Kern-Prozessor ab 3,3 GHz pro Kern)
- mind. 2 GB RAM (empfohlen: 4 GB RAM)

Für folgende Leistungsmerkmale werden 4 GB RAM benötigt:

- FAX als PDF
- Mehr als 500 Benutzer
- OpenScape Business Contact Center
- Gateview
- XMPP
- LAN-Anschluss mit mind. 100 Mbit/s

- DVD-Laufwerk, Tastatur, Maus
- Bildschirmauflösung: 1024x768 oder höher
- die Größe der Festplatte ist abhängig von der Anzahl der Benutzer:

Anzahl Benutzer	Größe der Festplatte
Bis 50 Benutzer	60 GB oder mehr
Bis 100 Benutzer	100 GB oder mehr
Bis 500 Benutzer	200 GB oder mehr
OpenScape Business Contact Center	200 GB oder mehr
Mehr als 500 Benutzer	500 GB oder mehr

Werden die Mindestvoraussetzungen unterschritten, ist die Installation zwar möglich, im Betrieb kann es aber zu Problemen kommen.

Software

Für die Installation des Linux-Betriebssystems auf dem Server-PC wird die Linux-Version **SLES 12 SP5 64 Bit** benötigt.

Beim Kauf der OpenScape Business Kommunikationssoftware können Sie eine DVD oder .ISO-Datei mit dieser Linux-Version beziehen. Diese DVD oder .ISO-Datei darf nur zusammen mit der Kommunikationssoftware genutzt werden.

Einige PC-Hersteller bieten für ihre Server-PC-Modelle eigene, für diese Modelle optimierte Linux-Installationsdatenträger an. Diese können verwendet werden, wenn sie die Linux-Version SLES 12 SP5 64 Bit enthalten.

Halten Sie die Linux-DVD oder .ISO-Datei bei der Installation der OpenScape Business Kommunikationssoftware bereit, da ggf. Software-Pakete (RPM) von dieser DVD nachinstalliert werden müssen, die für die Kommunikationssoftware benötigt werden.

SLES 12 SP5 64 Bit Zertifizierung

Der Server-PC muss für SLES 12 SP5 64 Bit zertifiziert sein.

Novell bietet den PC-Herstellern mit "YES" ein Zertifizierungsprogramm für die Zertifizierung ihrer Server-PCs an. Die Ergebnisse sind im Internet verfügbar unter:

<http://developer.novell.com/yesssearch/Search.jsp>

Liegt keine Zertifizierung vor, muss beim PC-Hersteller nachgefragt werden, ob der Server-PC für SLES 12 SP5 64 Bit tauglich ist. Ist trotz Zertifizierung zusätzliche Hardware eingebaut (z.B. Netzwerkkarte oder Grafikkarte), die nicht SLES 12 SP5 64 Bit kompatibel ist, muss beim Kartenhersteller ein passender Treiber beschafft werden. Sollte kein Treiber verfügbar sein, ist die Karte gegen ein SLES 12 SP5 64 Bit kompatibles Modell auszutauschen.

Registrierung bei Novell

Die Installation und der Betrieb von SLES 12 SP5 64 Bit ist zwar ohne Registrierung bei Novell möglich, aber um Sicherheits-Patches und Software-Updates zu erhalten, ist eine Registrierung bei Novell notwendig. Dafür müssen Sie mit Hilfe des Activation Codes ein Kundenkonto bei Novell erstellen (siehe

auch [Updates auf Seite 179](#)). Es wird empfohlen, das Kundenkonto vor der Linux-Installation einzurichten.

Einen Novell Activation Code (Registrierungscode) können Sie über die Bestellposition "OpenScape Business SLES Upgrade key" beziehen.

Infrastruktur

An das interne Netz werden folgende Bedingungen gestellt:

- LAN mit min. 100 Mbit/s und IPv4
- Einheitliche Zeitbasis (z.B. über NTP-Server)
- feste IP-Adresse des Server-PC

Internetzugang

Der Server-PC benötigt einen Internet-Zugang für:

- Registrierung bei Novell
- 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
- Remote Service (SSDP)/RSP.servicelink

Netzwerk-Konfiguration

Während der Linux-Installation werden Angaben zur Netzwerkkonfiguration abgefragt. Deshalb ist es sinnvoll vor der Netzwerkkonfiguration ein IP-Adress-Schema zu erstellen, das alle Netzwerkkomponenten und deren IP-Adressen enthält.

Nachfolgend finden Sie ein Beispiel eines IP-Adress-Schemas mit dem IP-Adressband 192.168.5.x. Die fett gekennzeichneten Parameter sind die minimalen Pflichtangaben während der Linux-Installation.

Parameter	Beispielwerte
externer DHCP-Server oder Linux-DHCP-Server	DHCP-Server des Internet-Routers (extern)
DHCP-Adressbereich	192.168.5.50 bis 192.168.5.254
Subnetzmaske des Netzwerks bzw. des Netzwerksegments	255.255.255.0
Feste IP-Adresse der Linux-Servers IP-Adresse muss außerhalb des DHCP-Adressbereichs liegen.	192.168.5.10
Internet-Router	192.168.5.1
Server mit fester IP-Adresse (optional), z.B. E-Mail-Server	192.168.5.20
Clients mit fester IP-Adresse (optional) IP-Adresse muss außerhalb des DHCP-Adressbereichs liegen.	192.168.5.1 bis 192.168.5.49

Installation des Linux-Servers

Installation in einer virtuellen Umgebung

Parameter	Beispielwerte
Standard-Gateway , z. B. der Internet-Router	192.168.5.1
DNS-Server , z. B. der Internet-Router	192.168.5.1
Domänenname bei Verwendung eines DNS-Servers , z. B. der Internet-Domänenname	customer.com
Host-Name von OpenScape Business Der Name kann frei gewählt werden, sollte jedoch mit dem Netzwerkadministrator abgestimmt sein.	comm_server

Liegen die Daten des Netzwerks zum Zeitpunkt der Installation noch nicht vor, sollte das Netzwerk mit Daten dieses Beispiel-Netzwerks eingerichtet werden.

Die Netzwerkdaten können nach der erfolgreichen Linux-Installation jederzeit über YaST geändert und an das Netzwerk angepasst werden.

Ein Überspringen der Netzwerkkonfiguration wird nicht empfohlen, da die nachfolgende Installation von OpenScape Business ohne ein vollständig eingerichtetes Netzwerk nicht erfolgreich durchgeführt werden kann.

8.2 Installation in einer virtuellen Umgebung

Die Kommunikationssoftware kann in einer virtuellen Umgebung laufen.

Für eine virtuelle Umgebung 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.

Für die Lizenzierung in einer virtuellen Umgebung wird für den Softswitch anstelle der MAC-Adresse des Server-PCs eine Advanced Locking ID generiert und verwendet.

Es ist folgende Virtualisierungssoftware freigegeben:

- Details über veröffentlichte VMware vSphere Versionen einschl. der neuesten Patches finden Sie in den OpenScape Business Versionshinweisen.
für die Hardware-Anforderungen an den physikalischen Server-PC siehe "VMware Compatibility Guide" und "VMware Resource Management Guide" unter www.vmware.com.

Zur Ermittlung der Hardware-Anforderungen an den physikalischen Server-PC bietet VMware auf der Internet-Homepage unter <http://www.vmware.com/guides> „Compatibility Guides“ eine Online-Suchfunktion zu zertifizierter und getesteter Hardware an.

Richtlinien zur Bereitstellung von Datenträgern sind zu finden in https://pubs.vmware.com/vsphere-50/index.jsp?topic=%2Fcom.vmware.vsphere.vm_admin.doc_50%2FGUID-81629CAB-72FA-42F0-9F86-F8FD0DE39E57.html

- Windows Server (2008 R2, 2012, 2012 R2) Hyper-V, einschl. der neuesten Patches.

Informationen zu den Hardware-Anforderungen des physischen Server-PCs finden Sie unter technet.microsoft.com.

Sie finden alle nötigen Informationen über Hyper-V im Abschnitt Library -> Windows Server 2012 R2 (oder Ihrem aktuellen Windows-Serversystem) -> Server Roles and Technologies -> Hyper V auf der Microsoft Technet-Seite.

Die Beschreibung der Installation und Konfiguration der Virtualisierungssoftware ist nicht Bestandteil dieser Dokumentation. Die Installation von Linux und der Kommunikationssoftware in einer virtuellen Umgebung verhält sich genauso wie die Installation direkt auf dem Server-PC.

Für Linux und die Kommunikationssoftware sind in der virtuellen Umgebung folgende Mindestvoraussetzungen zu konfigurieren:

Parameter	VM-Einstellungen
Guest Operating System	SLES 12 SP5 64 Bit
VM HD Capacity	Bis 50 Benutzer: 60 GB oder mehr Bis 100 Benutzer: 100 GB oder mehr Bis 500 Benutzer: 200 GB oder mehr OpenScape Business Contact Center: 200 GB oder mehr Ab 500 Benutzer: 500 GB oder mehr
Virtual Disk Mode	Standard
Virtual Disk Format Type	Thin Provisioning (dynamic HD Capacity) or Thick Provisioning (fixed HD Capacity)
vCPUs	2 4 für OpenScape Business Contact Center oder mehr als 500 Benutzer
vCPUs Shares (High/Normal)	Hoch
vCPU Reservation	2 GHz
vCPU Limit	Unbegrenzt
VM Memory	2 GB 4 GB für: - FAX als PDF - OpenScape Business Contact Center - Gate View - XMPP 8 GB für: - Mehr als 500 Benutzer
VM Memory Shares (High/Normal)	Normal

Parameter	VM-Einstellungen
VM Memory Reservation	4 GB
VM Memory Limit	Unbegrenzt
Anzahl vNICs	1
VMware Manual MAC Used	NEIN
Virtual Network Adapter Support	YES, vmxnet3-Treiber
VMware Tools Installation	JA

Die VM (Virtual Machine) darf die CPU bis zu 70% auslasten, Werte darüber können zu Fehlverhalten führen.

Folgende VMware vSphere Leistungsmerkmale werden unterstützt:

- Thin Provisioning
- High Availability (HA)
- VMotion
- Data Recovery (VDR)
- DRS (VMotion automatisiert)
- Storage VMotion

Folgende VMware vSphere Leistungsmerkmale werden nicht unterstützt:

- Fault Tolerance

Folgende Microsoft Hyper-V Leistungsmerkmale werden unterstützt:

- Thin Provisioning
- High Availability (HA)
- Live-Migration
- Datenwiederherstellung

Der Bildschirmschoner für die virtuelle Umgebung ist zu deaktivieren.

8.2.1 VM Co-Residency und QoS-Richtlinie

Diese VM Co-Residency und QoS-Richtlinie beschreibt die Verantwortlichkeiten der für die Bereitstellung der Unify-VMs und die Verwaltung der virtuellen Umgebung zuständigen Parteien. Diese gelten für die Bereitstellung von Unify-VMs in konsolidierten Netzwerken und Hardwareressourcen:

- Die für die Bereitstellung der Unify-VMs und die Verwaltung der virtuellen Umgebung zuständigen Parteien verpflichten sich, die vorgegebenen Leistungskriterien zu erfüllen. Unsicherheiten können durch Pre-Deployment-Tests, Baselineing und Einhaltung der Konfigurationsregeln für Unify-VMs sowie des Resource Guides (VM R&C) – einschließlich dieser Richtlinie – minimiert werden.
- VMs mit Echtzeit- und unternehmenskritischen Unify-Anwendungen müssen von anderen Anwendungen im Routing- und Vermittlungsnetzwerk abgeschirmt werden, um sicherzustellen, dass für Sprach- und Videodaten genügend Bandbreite und ausreichender Schutz vor Latenz und Jitter vorhanden ist.
- VMs mit Echtzeit- und unternehmenskritischen Unify-Anwendungen müssen von anderen Anwendungen abgeschirmt werden, wenn der

Virtualisierungshost Rechen-, Speicher- und Netzwerk-Hardware mit virtuellen Maschinen, auf denen mehrere Anwendungen laufen, teilt (d.h. die Unify-Echtzeit-Anforderungen sind nicht planbar).

- Die Einhaltung des Unify-Regelwerks für die Konfiguration von VMs und Ressourcen (z.B. physische/virtuelle Hardware-Dimensionierung, Co-Residency-Richtlinie etc.) ist notwendig, um sicherzustellen, dass Unify-VMs die benötigten CPU-, RAM-, Speicherkapazitäten und Storage-/Netzwerkleistungsreserven erhalten.
- Unify-VMs dürfen nicht mit Drittanbieter-VMs auf derselben Hardware installiert werden, wenn die Ressourcenanforderungen der Drittanbieter VMs nicht klar definiert sind.
- Die Hardware des Hosts wird kontinuierlich überwacht (z.B. durch vCenter). Die CPU-Auslastung sollte unter 80 % liegen und der %RDY-Wert bei maximal 5 %.
- Die vom Arbeitsspeicher, Speicher und Netzwerk (einschließlich Speichernetzwerk) benötigte Bandbreite darf die Kapazität der Host-Hardware nicht überschreiten (keine Überbelegung).
- Auch wenn der Hostprozessor Hyper-Threading unterstützt und diese Funktion aktiviert ist, wird ein physischer Kern immer nur einfach gezählt.
- vCPU-Anteile werden so konfiguriert, dass für unternehmenskritische Unify-VMs (einschließlich Echtzeit-VMs) immer genügend CPU-Zeit zur Verfügung steht.
- Kunden sind selbst für die Einhaltung dieser Anforderungen verantwortlich, insbesondere dann, wenn VMs verschoben werden (z. B. durch manuelle Neukonfiguration der CPU-Anteile einer VM, wenn diese auf einen anderen VM-Host oder in einen anderen Ressourcenpool verschoben wurde).
- Disaster Recovery-Pläne müssen auch die zusätzlichen Ressourcen berücksichtigen, die für einen erfolgreichen Failover zum Failover-Standort (Rechenzentrum 2) erforderlich sind.

8.2.2 Zeitsynchronisation des Gastbetriebssystems Linux

Die Zeitsynchronisation (einheitliche Zeitbasis von Datum und Uhrzeit) zwischen Hostbetriebssystem VMware vSphere oder Microsoft Hyper-V und Gastbetriebssystem Linux muss deaktiviert werden. Die einheitliche Zeitbasis sollte das Gastbetriebssystem über einen NTP-Server bekommen.

8.2.2.1 Wie Sie die Zeitsynchronisation für das Gastbetriebssystem Linux in VMWare konfigurieren

Schritt für Schritt

- 1) Klicken Sie mit dem VMware Client **vSphere Client** mit der rechten Maustaste auf das Gastbetriebssystem Linux und wählen Sie den Menüpunkt **Edit Settings**.
- 2) Deaktivieren Sie unter den **Virtual Machine Properties** im Register **Options** unter dem Eintrag **VMware Tools** im Bereich **Advanced** die Option **Synchronize guest time with host**.

- 3) Ändern Sie für das Gastbetriebssystem Linux die NTP-Einstellungen in der Datei `./etc/ntp.conf` wie folgt anhand der fett gedruckten Parameter:

```
*****  
  
...  
  
tinker panic 0  
  
# server 127.127.1.0  
  
# local clock (LCL)  
  
# fudge 127.127.1.0 stratum 10  
  
# LCL is unsynchronized  
  
...  
  
server 0.de.pool.ntp.org iburst  
  
restrict 0.de.pool.ntp.org  
  
restrict 127.0.0.1  
  
restrict default kod nomodify notrap  
  
...  
  
*****
```

Anmerkung: Der NTP-Server **de.pool.ntp.org** ist beispielhaft und muss ggfs. durch eine von dem Gastbetriebssystem Linux erreichbare NTP-Server-Adresse ersetzt werden.

8.3 Linux-Sicherheitsaspekte und RAID-Verbund

Die Beachtung der Linux-Sicherheitsaspekte und die Verwendung eines RAID-Verbunds erhöht die Sicherheit des Linux-Servers.

Firewall

Beim Anschluss an das Internet ist 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. Es sind alle Dienste für die Kommunikationssoftware freigegeben bis auf CSTA (CSTA-Schnittstelle) und SSH (Secure Shell).

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](#) auf Seite 277 in der Installationsanleitung zu OpenScape Business S oder OpenScape Business UC Booster Server).

Virens Scanner

Ein Virens Scanner ist nicht im Installationsumfang von Linux enthalten. Es sollte ein Virens Scanner installiert werden. Mehr Informationen erhalten Sie bei Bedarf in den Versionshinweisen der Kommunikationssoftware.

Um eventuellen, durch den Einsatz eines Virens Scanners resultierenden Performance-Problemen vorzubeugen, sind die regelmäßigen Festplatten-Scans auf Zeiten zu legen, in denen die Kommunikationssoftware nicht oder nur geringfügig genutzt wird.

Intrusion Detection System (AppsArmor)

Die Installationsroutine des Application Servers nimmt keine Anpassungen am Linux Intrusion Detection System (AppsArmor) vor. Die Standardeinstellungen der Linux-Installation werden übernommen. Weitere Einstellungen sind für den Betrieb der Kommunikationssoftware nicht erforderlich.

Während der Installation des Softswitches wird das Linux Intrusion Detection System (AppsArmor) aktualisiert und aktiviert. Weitere Einstellungen sind für den Betrieb der Kommunikationssoftware nicht erforderlich.

Ausfallsicherheit

Empfehlungen zur Erhöhung der Ausfallsicherheit (Redundancy):

- zwei Festplatten im RAID1-Verbund.
- zweites Spannungsnetzteil für den Linux-Server
- Unterbrechungsfreie Spannungsversorgung

Bei Verwendung von IP-Telefonen ist darauf zu achten, dass die LAN-Switches und IP-Telefone ebenfalls über eine unterbrechungsfreie Spannungsversorgung geführt werden.

RAID1-Verbund

Bei einem RAID1-Verbund wird der Inhalt der ersten Festplatte auf die zweite Festplatte gespiegelt. Fällt eine Festplatte aus, läuft das System auf der zweiten Festplatte weiter.

Ein RAID-Verbund ist als Software-RAID oder als Hardware-RAID (BIOS RAID oder HW-RAID-Controller) möglich.

Für die Besonderheiten bei der Installation mit einem Software-RAID siehe .

Ein Hardware-RAID erfordert in vielen Fällen einen eigenen Treiber, der nicht im Linux-Betriebssystem enthalten ist. Dieser Treiber wird vom Hersteller bereitgestellt und muss entsprechend den Hersteller-Vorgaben installiert werden. Ist der Treiber nicht zur Linux-Version kompatibel oder wird kein Linux-Treiber angeboten, kann der Hardware-RAID nicht eingesetzt werden. Die Beschreibung von Hardware-basierten RAID-Systemen ist nicht Bestandteil dieser Dokumentation. Kontaktieren Sie in diesem Fall für Linux-Treiber und Konfiguration den Hersteller.

8.4 Erstinbetriebnahme ohne Software-RAID

Die Erstinbetriebnahme des Linux-Servers ohne Software-RAID umfasst die Linux-Installation und -Konfiguration unter Berücksichtigung, dass kein Software-RAID genutzt werden soll.

Die für die Kommunikationssoftware nötigen Einstellungen werden während der Installation und Konfiguration getroffen.

Linux-Partitionen

Die Festplatte ist während der Erstinbetriebnahme folgendermaßen zu partitionieren:

Partition	Typ	Größe	Filesystem	Mount	Hinweis
1. Partition	Primary Partition	2 GB	Swap	swap	entspricht der Größe des Arbeitsspeichers
2. Partition	Primary Partition	15 GB	Ext3	/	für das Linux-Betriebssystem
3. Partition	Primary Partition	Rest ¹	Ext3	/home	Für die Kommunikationssoftware

Anmerkung: Die Installationsroutine der Kommunikationssoftware fragt diese Partitionsgrößen ab und verweigert u.U. die Installation.

Anmerkung: Einige Server-PCs benötigen eine zusätzliche Boot-Partition. Falls Linux eine Boot-Partition vorschlägt, sollte diese in der vorgeschlagenen Größe übernommen werden.

8.4.1 SLES 12 SP5 ohne Software-RAID installieren und konfigurieren

Voraussetzungen

Das BIOS-Setup des Linux-Servers ist so eingestellt, dass der Server von DVD oder .ISO-Datei auf USB-Stick bootet.

Für die Registrierung bei Novell ist ein Internet-Zugang und der Aktivierungscode vorhanden.

Schritt für Schritt

- 1) Legen Sie die SLES 12 DVD in das DVD-Laufwerk ein oder stecken die .ISO-Datei auf einem USB-Stick in einen USB-Port und booten Sie von der DVD oder .ISO-Datei. Es erscheint das Startfenster der Linux-Installation.
- 2) Wählen Sie den Menüpunkt **Installation** aus und bestätigen Sie mit der Eingabetaste.

¹ Bis 50 Benutzer mind. 40 GB - bis 100 Benutzer mind. 80 GB - bis 500 Benutzer mind. 180 GB - bei OpenScape Business Contact Center mind. 180 GB - über 500 Benutzer mind. 480 GB

- 3) Wählen Sie im Fenster **Language, Keyboard and License Agreement** die Ländereinstellungen für das Linux-Betriebssystem:
 - a) Wählen Sie als Oberflächensprache in der Aufklappliste **Language** die Sprache **English (US)** aus.
 - b) Wählen Sie für die Tastaturbelegung in der Aufklappliste **Keyboard Layout** das gewünschte Land aus.
- 4) Lesen Sie sich die Lizenzvereinbarung durch und akzeptieren Sie diese, indem Sie das Kontrollkästchen **I Agree to the License Terms** aktivieren. Klicken Sie anschließend auf **Next**.
- 5) Klicken Sie im Fenster **Registration** auf **Register System via scc.suse.com**, geben Sie Ihre E-Mail-Adresse und den Registrierungscode ein und klicken Sie auf **Weiter**.

: Wenn Sie die Registrierung überspringen möchten, wählen Sie **Registrierung überspringen**, klicken Sie im daraufhin angezeigten Fenster **Warnung** auf **OK** und anschließend auf **Weiter**. Wenn Sie die Registrierung überspringen, haben Sie keinen Zugriff auf die Update-Repositories. Sie können die Registrierung aber auch nach der Installation vornehmen oder den Kundendienst besuchen.

- 6) Klicken Sie im Fenster **Add On Product** auf **Network Configuration**.

Anmerkung: Wenn Sie das Netzwerk später konfigurieren möchten, klicken Sie auf **Weiter**.

- 7) Konfigurieren Sie im Fenster **Network Settings** die Netzwerkkarte.
 - a) Wählen Sie im Fenster **Overview** die gewünschte Netzwerkkarte aus. Der MAC-Adresse der hier ausgewählten Netzwerkkarte werden später bei der Lizenzierung die Lizenzen zugeordnet. Klicken Sie auf **Bearbeiten**.
 - b) Aktivieren Sie das Optionsfeld **Statically assigned IP Address**.
 - c) Geben Sie unter **IP Address** die Ihnen zugewiesene IP-Adresse des Linux-Servers ein, (z. B. 192.168.5.10).
Die IP-Adresse muss zu dem IP-Adressen-Schema Ihres internen Netzes passen und darf keinem bestehenden Netzwerk-Client zugewiesen sein, da es sonst zu einem IP-Adressen-Konflikt kommt.
 - d) Geben Sie unter **Subnet Mask** die Ihnen zugewiesene Subnetzmaske des Linux-Servers ein, (z. B. 255.255.255.0).
Die Subnetzmaske muss zu dem IP-Adressen-Schema Ihres internen Netzes passen.
 - e) Geben Sie unter **Hostname** den zugewiesenen Hostnamen des Linux-Servers ein (z. B. OSBiz-Booster).
Der Hostname muss zu dem Hostname-Schema Ihres internen Netzes passen und darf keinem bestehenden Netzwerk-Client zugewiesen sein, da es sonst zu einem Hostname-Konflikt kommt.
 - f) Klicken Sie anschließend auf **Next**.

- 8) Geben Sie den DNS-Server und das Standard-Gateway an:
 - a) Klicken Sie im Fenster **Network Settings** auf die Registerkarte **Hostname/DNS**.
 - b) Geben Sie den Hostnamen des DNS-Servers unter **Hostname** ein.
Der Hostname muss zu dem Hostname-Schema Ihres internen Netzes passen und darf keinem bestehenden Netzwerk-Client zugewiesen sein, da es sonst zu einem Hostname-Konflikt kommt.
 - c) Geben Sie den Domännennamen des DNS-Servers unter **Domänenname** ein.
Der Domänenname muss eindeutig sein, da es sonst zu einem Domännennamen-Konflikt kommen würde.
 - d) Geben Sie unter **Name Server 1** die IP-Adresse des DNS-Servers ein.
Ist im internen Netz kein DNS-Server vorhanden, tragen Sie hier die IP-Adresse des Internet-Routers ein (z. B. 192.168.5.1).
 - e) Klicken Sie im Fenster **Network Settings** auf das Register **Routing**.
 - f) Geben Sie unter **Default Gateway** die IP-Adresse des Internet-Routers ein (zum Beispiel 192.168.5.1).
- 9) Klicken Sie auf **Next**.
- 10) Klicken Sie unter **Add On Product** auf **Next**.
- 11) Wählen Sie im Fenster **System Role** die Option **Default System** aus, und klicken Sie auf **Next**.
- 12) Wählen Sie im Fenster **Suggested Partitioning** die Option **Expert Partitioner...** aus.
- 13) Löschen Sie alle vorbelegten Partitionen (sda1, sda2 usw.)
Klicken Sie mit der rechten Maustaste auf jede Partition, wählen Sie **Delete** und bestätigen Sie das Löschen mit einem Klick auf **Yes**.
- 14) Richten Sie eine Swap-Partition ein.
 - a) Klicken Sie auf Device `/dev/sda` und wählen Sie **Add Partition** aus.
 - b) Aktivieren Sie das Optionsfeld **Primary Partition** und klicken Sie anschließend auf **Next**.
 - c) Geben Sie unter **Custom Size** die Größe der Swap-Partition an und klicken Sie anschließend auf **Next**.
In der Regel entspricht die Swap-Partition der Größe des Arbeitsspeichers. Zum Beispiel mit 4GB RAM sollte die Swap-Partition mit der Eingabe `4GB` auf 4 GB eingestellt werden. Die Mindestgröße der Swap-Partition beträgt 2 GB und die empfohlene Größe 4 GB.
 - d) Wählen Sie im Fenster **Add Partition on /dev/sda** die Rolle **Swap** aus, und klicken Sie auf **Finish**

- 15) Richten Sie die Partition für das Linux-Betriebssystem ein.
 - a) Klicken Sie auf Device `/dev/sda` und wählen Sie **Add Partition** aus.
 - b) Aktivieren Sie das Optionsfeld **Primary Partition** und klicken Sie anschließend auf **Next**.
 - c) Geben Sie unter **Custom Size** die Größe der Partition an (z.B. sind 15 GB ausreichend - Eingabe: 15GB) und klicken Sie auf **Next**.
Die Mindestgröße der Partition des Linux-Betriebssystems beträgt 15 GB und die empfohlene 20 GB.
 - d) Wählen Sie im Fenster **Add Partition on /dev/sda** die Rolle **Operating System** aus, und klicken Sie auf **Next**
 - e) Wählen Sie unter **Format partition** die Option **Ext3** oder **Ext4** aus, wählen Sie unter **Mount partition** die Option `/` aus und klicken Sie auf **Finish**.
- 16) Richten Sie die Partition für die Kommunikationssoftware ein.
 - a) Klicken Sie auf Device `/dev/sda` und wählen Sie **Add Partition** aus.
 - b) Aktivieren Sie das Optionsfeld **Primary Partition**.
 - c) Geben Sie unter **Custom Size** die maximale Größe ein, und klicken Sie auf **Next**.
Die Mindestgröße der Partition für die Kommunikationssoftware beträgt 40 GB.
 - d) Wählen Sie im Fenster **Add Partition on /dev/sda** die Rolle **Data and ISV Applications** aus, und klicken Sie auf **Next**
 - e) Wählen Sie unter **Format partition** die Option **Ext3** aus, wählen Sie unter **Mount partition** die Option `/home` aus, klicken Sie auf **Finish** und auf **Accept**.
- 17) Klicken Sie im Fenster **Suggested Partitioning** auf **Next**.
- 18) Wählen Sie im Fenster **Clock and Time Zone** die korrekte Region und Zeitzone aus.
Stellen Sie gegebenenfalls das Datum und die Uhrzeit ein, indem Sie auf die Schaltfläche **Other Settings** klicken und dann auf **Next**.
- 19) Geben Sie im Fenster **Local Users** einen Benutzer und ein Kennwort ein, und klicken Sie auf **Next**.
- 20) Geben Sie im Fenster **Password for the System Administrator "root"** das Passwort für den Systemadministrator mit dem Profil "root" in die Felder **Password for the root User** und **Confirm Password** ein und klicken Sie auf **Next**.
Das Kennwort sollte den gebräuchlichen Sicherheitsrichtlinien entsprechen. Es sollte mindestens 8 Zeichen, mindestens einen Kleinbuchstaben, mindestens einen Großbuchstaben, mindestens eine Zahl und mindestens ein Sonderzeichen enthalten.
- 21) Klicken Sie im Fenster **Installation Settings** auf **Install**, und bestätigen Sie die Installation, indem Sie erneut auf **Install** klicken.
Das Fenster **Installation Settings** bietet eine Übersicht über die Komponenten, die installiert werden. Vor dem Abschluss der Installation können Sie hier eventuell nötige Änderungen vornehmen.

Nachdem der Installationsvorgang abgeschlossen wurde, wird der Computer auf dem installierten System neu gestartet. Nehmen Sie die DVD aus dem DVD-Laufwerk.

Um eine geeignete Bildschirmauflösung zu wählen:

- Klicken Sie in der Taskleiste auf **Anwendungen**.
- Klicken Sie dann im Menübaum **Einstellungen > Displays**.
- Klicken Sie im Fenster **Displays** auf das Feld **Unbekanntes Display**
- Wählen Sie im Pop-up-Fenster **Unbekanntes Display** die entsprechende Auflösung aus der Aufklappliste **Auflösung** aus und klicken Sie dann auf **Übernehmen**.
- Klicken Sie abschließend im Bestätigungs-Pop-up-Fenster auf **Änderungen beibehalten**.

Nächste Schritte

NTP-Server konfigurieren (für eine einheitliche Zeitbasis).

8.4.2 Wie Sie von SLES 11 auf SLES 12 SP5 aktualisieren

Voraussetzungen

OpenScape Business auf SLES 11 SP4

Anmerkung: Wenn eine ältere Version verwendet wird, ist vorher ein Upgrade auf SLES 11 SP4 erforderlich.

Dieses Kapitel beschreibt das Upgrade eines voll funktionsfähigen OpenScape Business Systems von SLES 11 SP4 auf SLES 12 SP5 mit einem parallelen Upgrade der OpenScape Business Version.

Wichtig: Während der Migration von SLES 11 SP4 auf SLES 12 SP5 sollte eine saubere/frische Installation statt des Upgrade-Mechanismus durchgeführt werden, auch wenn dies als Option angeboten wird.

Bei einer frischen Installation können Sie Ihr OpenScape Business Backup von der früheren Version in den neu installierten Systemen, die auf SLES 12 basieren, wiederherstellen.

Es wurde beobachtet, dass der Upgrade-Mechanismus Probleme bei einigen Einstellungen von Linux verursachen kann, die für die OpenScape Business Funktionalität kritisch sein können.

Bei Verwendung einer virtuellen Maschine (z. B. ESXi) sollte eine neue VM erstellt werden und die als SLES 11 SP4 verwendete VM sollte nicht verwendet werden. Andernfalls kann es zu zusätzlichen Problemen kommen, wenn das Host-BS (z. B. ESCi) sich über die installierte Linux-Version des Gasts beschwert (VM wird anfänglich für SLES 11 erstellt und führt jetzt SLES 12 aus).

Bei der Option einer sauberen/frischen Installation in der VM wird die ALI (Locking-ID) des Systems geändert und ein Rehost der alten Lizenz ist obligatorisch.

Schritt für Schritt

- 1) Sichern Sie alle OpenScape Business Server oder UC Booster Server Daten.
Befolgen Sie die Anweisungen in [Wie Sie eine Datensicherung durchführen](#)
- 2) Deinstallieren Sie OpenScape Business Server oder UC Booster Server.
Befolgen Sie die Anweisungen in [Wie Sie die Kommunikationssoftware deinstallieren](#)
- 3) Legen Sie die SLES 12 SP5 Installations-DVD ein und booten Sie.
- 4) Wählen Sie **Upgrade**.

Anmerkung: Es wird zur Installation des Pakets libpango-1_0-0-32bit aufgefordert, die während des Upgrades fehlgeschlagen ist. Sie können diese Meldung ignorieren. Die Installation wird erfolgreich fortgesetzt.

- 5) Nachdem das System-Upgrade auf SLES 12 SP5 abgeschlossen ist, installieren Sie eine OpenScape Business Server DVD-Version, die SLES 12 SP5 unterstützt.

Anmerkung: Verwenden Sie dieselbe Partitionierung in SLES 11 SP4. Außerdem muss das Dateisystem für SLES 11 und SLES 12 gleich sein, da die Sicherung sonst nicht mehr importiert werden kann.

- 6) Stellen Sie alle OpenScape Business Server-Daten wieder her.

8.4.3 Wie Sie von SLES 12 SP3 auf SLES 12 SP5 aktualisieren

Dieses Kapitel beschreibt das Upgrade eines voll funktionsfähigen OpenScape Business Systems von SLES 12 SP3 auf SLES 12 SP5. Dieses Upgrade kann ohne eine neuerliche Installation des OpenScape Business Systems durchgeführt werden.

Schritt für Schritt

- 1) Aktualisieren Sie SLES 12 SP3 auf SLES 12 SP4 nach den Anweisungen von Novell.
- 2) Aktualisieren Sie SLES 12 SP4 auf SLES 12 SP5 nach den Anweisungen von Novell.

Obwohl die Aktualisierung von SLES 12 SP3 auf SLES 12 SP5 ohne Neuinstallation des OpenScape Business Systems unterstützt wird, muss zuerst das Upgrade auf SLES 12 SP4 vorgenommen werden. Novell unterstützt das direkte Upgrade von SP3 auf SP5 nicht.

8.5 Erstinbetriebnahme mit Software-RAID

Die Erstinbetriebnahme des Linux-Servers mit Software-RAID umfasst die Linux-Installation und -Konfiguration unter Berücksichtigung, dass ein Software-RAID genutzt werden soll.

Gehen Sie folgendermaßen vor:

1) BIOS RAID deaktivieren (optional)

Wenn ein RAID-Verbund über einen Software-RAID eingerichtet werden soll, ist im BIOS ein ggf. auf dem Motherboard des Server-PC integriertes BIOS RAID zu deaktivieren.

2) SLES 12 SP5 mit Software-RAID installieren und konfigurieren

Die für die Kommunikationssoftware nötigen Einstellungen werden während der Installation und Konfiguration getroffen.

Linux-Partitionen

Die Festplatte ist während der Erstinbetriebnahme folgendermaßen zu partitionieren:

Partition	Typ	Größe	Filesystem	Mount	Bemerkung
1. Partition	Primary Partition	2 GB	Swap	swap	entspricht der Größe des Arbeitsspeichers
Partition 2	Primary Partition	15 GB	Ext4	Kein Mount Point	für das Linux-Betriebssystem
Partition 3	Primary Partition	Rest ²	Ext3	Kein Mount Point	Für die Kommunikationssoftware

Die Mount Points werden nach der Partitionierung bei der Einrichtung des RAID-Systems vergeben.

Anmerkung: Die Installationsroutine der Kommunikationssoftware fragt diese Partitionsgrößen ab und verweigert u.U. die Installation.

Anmerkung: Einige Server-PCs benötigen eine zusätzliche Boot-Partition. Falls Linux bei der Installation eine Boot-Partition vorschlägt, sollte diese in der vorgeschlagenen Größe übernommen werden.

² Bis 50 Benutzer mind. 40 GB - bis 100 Benutzer mind. 80 GB - bis 500 Benutzer mind. 180 GB - bei OpenScape Business Contact Center mind. 180 GB - über 500 Benutzer mind. 480 GB

8.5.1 Wie Sie das BIOS RAID deaktivieren

Voraussetzungen

Ein auf dem Motherboard des PCs integrierter RAID-Controller (BIOS RAID) ist vorhanden.

Schritt für Schritt

- 1) Starten Sie den PC neu. Während des Hochlaufens wird Ihnen angezeigt, ob der BIOS RAID aktiviert ist. Ist der BIOS RAID nicht aktiviert, springen Sie zu Schritt 3.
- 2) Deaktivieren Sie den aktiven BIOS RAID:
 - a) Drücken Sie während des Hochlaufens an geeigneter Stelle die Tastenkombination, um in das Setup des BIOS RAID zu gelangen. Die Kombination wird Ihnen während des Hochlaufens angezeigt (z.B. CTRL-M für LSI MegaRAID BIOS).
 - b) Löschen Sie die BIOS-RAID-Konfiguration. Beispiel für LSI MegaRAID BIOS: Management Menu > Configure > Configuration Menu > Clear Configuration.
 - c) Beenden Sie das Setup des BIOS RAID und starten Sie den PC neu.
- 3) Deaktivieren Sie die SATA RAID-Konfiguration im BIOS-Setup des PC:
 - a) Drücken Sie während des Hochlaufens an geeigneter Stelle die Taste, um in das BIOS-Setup des PC zu gelangen (z.B. F2 oder DEL).
 - b) Deaktivieren Sie den SATA RAID. Beispiel für ein Phoenix BIOS: Advanced > Advanced System Configuration > SATA RAID Disabled.
 - c) Speichern Sie Ihre Änderungen und verlassen Sie das BIOS-Setup des PC (z.B. mit Taste F10).
- 4) Starten Sie den PC neu.

Nächste Schritte

SLES 12 mit Software-RAID installieren und konfigurieren.

8.5.2 Wie Sie SLES 12 SP5 Software-RAID installieren und konfigurieren

Voraussetzungen

Ein evtl. vorhandener HW-RAID ist deaktiviert.

Das BIOS-Setup des Linux-Servers ist so eingestellt, dass der Server von DVD oder .ISO-Datei bootet.

Für die Registrierung bei Novell ist ein Internet-Zugang und der Aktivierungscode vorhanden.

Schritt für Schritt

- 1) Legen Sie die SLES 12 DVD in das DVD-Laufwerk ein oder stecken die .ISO-Datei auf einem USB-Stick in einen USB-Port und booten Sie von der DVD oder .ISO-Datei. Es erscheint das Startfenster der Linux-Installation.
- 2) Wählen Sie den Menüpunkt **Installation** aus und bestätigen Sie mit der Eingabetaste.

- 3) Wählen Sie im Fenster **Language, Keyboard and License Agreement** die Ländereinstellungen für das Linux-Betriebssystem:
 - a) Wählen Sie als Oberflächensprache in der Aufklappliste **Language** die Sprache **English (US)** aus.
 - b) Wählen Sie für die Tastaturbelegung in der Aufklappliste **Keyboard Layout** das gewünschte Land aus.
- 4) Lesen Sie sich die Lizenzvereinbarung durch und akzeptieren Sie diese, indem Sie das Kontrollkästchen **I Agree to the License Terms** aktivieren. Klicken Sie anschließend auf **Next**.
- 5) Klicken Sie im Fenster **Registration** auf **Register System via scc.suse.com**, geben Sie Ihre E-Mail-Adresse und den Registrierungscode ein und klicken Sie auf **Weiter**.

: Wenn Sie die Registrierung überspringen möchten, wählen Sie **Registrierung überspringen**, klicken Sie im daraufhin angezeigten Fenster **Warnung** auf **OK** und anschließend auf **Weiter**. Wenn Sie die Registrierung überspringen, haben Sie keinen Zugriff auf die Update-Repositories. Sie können die Registrierung aber auch nach der Installation vornehmen oder den Kundendienst besuchen.

- 6) Klicken Sie im Fenster **Add On Product** auf **Network Configuration**.

Anmerkung: Wenn Sie das Netzwerk später konfigurieren möchten, klicken Sie auf **Weiter**.

- 7) Konfigurieren Sie im Fenster **Network Settings** die Netzwerkkarte.
 - a) Wählen Sie im Fenster **Overview** die gewünschte Netzwerkkarte aus. Der MAC-Adresse der hier ausgewählten Netzwerkkarte werden später bei der Lizenzierung die Lizenzen zugeordnet. Klicken Sie auf **Bearbeiten**.
 - b) Aktivieren Sie das Optionsfeld **Statically assigned IP Address**.
 - c) Geben Sie unter **IP Address** die Ihnen zugewiesene IP-Adresse des Linux-Servers ein, (z. B. 192.168.5.10).

Die IP-Adresse muss zu dem IP-Adressen-Schema Ihres internen Netzes passen und darf keinem bestehenden Netzwerk-Client zugewiesen sein, da es sonst zu einem IP-Adressenkonflikt kommt.
 - d) Geben Sie unter **Hostname** den zugewiesenen Hostnamen des Linux-Servers ein (z. B. OSBiz-Booster).

Der Hostname muss zu dem Hostname-Schema Ihres internen Netzes passen und darf keinem bestehenden Netzwerk-Client zugewiesen sein, da es sonst zu einem Hostname-Konflikt kommt.
 - e) Geben Sie unter **Subnet Mask** die Ihnen zugewiesene Subnetzmaske des Linux-Servers ein, (z. B. 255.255.255.0).

Die Subnetzmaske muss zu dem IP-Adressen-Schema Ihres internen Netzes passen.
 - f) Klicken Sie anschließend auf **Next**.

- 8) Geben Sie den DNS-Server und das Standard-Gateway an:
 - a) Klicken Sie im Fenster **Network Settings** auf das Register **Host name/ DNS**.
 - b) Geben Sie den Hostnamen des DNS-Servers unter **Hostname** ein.
Der Hostname muss zu dem Hostname-Schema Ihres internen Netzes passen und darf keinem bestehenden Netzwerk-Client zugewiesen sein, da es sonst zu einem Hostname-Konflikt kommt.
 - c) Geben Sie den Domännennamen des DNS-Servers unter **Domänenname** ein.
Der Domänenname muss eindeutig sein, da es sonst zu einem Domännennamen-Konflikt kommen würde.
 - d) Geben Sie unter **Name Server 1** die IP-Adresse des DNS-Servers ein.
Ist im internen Netz kein DNS-Server vorhanden, tragen Sie hier die IP-Adresse des Internet-Routers ein (z. B. 192.168.5.1).
 - e) Klicken Sie im Fenster **Network Settings** auf das Register **Routing**.
 - f) Geben Sie unter **Default Gateway** die IP-Adresse des Internet-Routers ein (zum Beispiel 192.168.5.1).
- 9) Klicken Sie auf **Next**.
- 10) Klicken Sie unter **Add On Product** auf **Next**.
- 11) Wählen Sie im Fenster **System Role** die Option **Default System** aus, und klicken Sie auf **Next**.
- 12) Wählen Sie im Fenster **Suggested Partitioning** die Option **Expert Partitioner...** aus.
- 13) Partitionieren Sie die beiden Festplatten:
 - a) Navigieren Sie im Menübaum **System View** zu **Hard Disks > sda** (erste Festplatte des Software-RAID).
 - b) Löschen Sie alle vorbelegten Partitionen (sda1, sda2, usw.), indem Sie die Partition markieren, auf **Delete** klicken und den Löschvorgang mit **Yes** bestätigen.
 - c) Partitionieren Sie die erste Festplatte über die Partition Schaltfläche **Add Partition**.

Verwenden Sie dabei folgende Daten:

1. Partition	Primary Partition	2 GB	Rolle: Swap Format Swap Mount Point = swap, fstab Option = Devicename
--------------	-------------------	------	--

Partition 2	Primary Partition	0,5 GB	Rolle: Betriebssystem Format Ext4 Mount Point = /boot Anmerkung: Diese Partition darf nur im ersten Laufwerk erstellt werden.
Partition 3	Primary Partition	15 GB	Rolle: Betriebssystem Format Ext4 no Mount Point
Partition 4	Primary Partition	Rest	Rolle: Data and ISV Applications Format Ext4 no Mount Point

- d) Navigieren Sie im Menübaum **System View** zu **Hard Disks > sdb** (zweite Festplatte des Software-RAID).
- e) Führen Sie die Schritte [13.b](#) auf Seite 175 und [13.c](#) auf Seite 175 genauso für die zweite Festplatte durch.

Anmerkung: Auf der zweiten Festplatte muss keine Startpartition erstellt werden.

- 14)** Treffen Sie die Software-RAID-Einstellungen:
- a) Wählen Sie den Menüpunkt **RAID** und klicken Sie auf **Add RAID**.
 - b) Wählen Sie **RAID 1 (Mirroring)** aus.
 - c) Markieren Sie im linken Bereich **Available Devices** die beiden Partitionen sda3 und sdb2 und übernehmen Sie diese mit **Add** in den rechten Bereich **Selected Devices**.
 - d) Klicken Sie auf **Next**.
 - e) Bestätigen Sie bei der Chunk-Größe den Default-Wert mit **Next**.
 - f) Wählen Sie im nächsten Fenster **Operating System** aus, und klicken Sie auf **Next**.
 - g) Wählen Sie im nächsten Fenster für das erste RAID-Device (/dev/md0) **Ext4** als Format und als Mount Point "/" aus, und klicken Sie auf **Finish**.
 - h) Klicken Sie erneut auf **Add Raid**.
 - i) Wählen Sie **RAID 1 (Mirroring)** aus.
 - j) Markieren Sie im linken Bereich **Available Devices** die beiden Partitionen sda4 und sdb3 und übernehmen Sie diese mit **Add** in den rechten Bereich **Selected Devices**.
 - k) Klicken Sie auf **Next**.
 - l) Bestätigen Sie bei der Chunk-Größe den Default-Wert mit **Next**.
 - m) Wählen Sie im nächsten Fenster **Data and ISV Applications** aus, und klicken Sie auf **Next**.
 - n) Wählen Sie im nächsten Fenster für das zweite RAID-Device (/dev/md1) **Ext4** als Format und als Mount Point „/home“ aus, und klicken Sie auf **Finish**.
- 15)** Klicken Sie auf **Accept** und auf **Next**.
Die Partitionierungsdaten werden gespeichert, die Partitionierung der Festplatte erfolgt später.
- 16)** Wählen Sie im Fenster **Clock and Time Zone** die korrekte Region und Zeitzone aus.
Stellen Sie gegebenenfalls das Datum und die Uhrzeit ein, indem Sie auf die Schaltfläche **Other Settings** klicken und dann auf **Next**.
- 17)** Geben Sie im Fenster **Local Users** einen Benutzer und ein Kennwort ein, und klicken Sie auf **Next**.
- 18)** Geben Sie im Fenster **Password for the System Administrator "root"** das Passwort für den Systemadministrator mit dem Profil "root" in die Felder **Password for the root User** und **Confirm Password** ein und klicken Sie auf **Next**.
Das Kennwort sollte den gebräuchlichen Sicherheitsrichtlinien entsprechen. Es sollte mindestens 8 Zeichen, mindestens einen Kleinbuchstaben, mindestens einen Großbuchstaben, mindestens eine Zahl und mindestens ein Sonderzeichen enthalten.
- 19)** Klicken Sie im Fenster **Installation Settings** auf **Install**, und bestätigen Sie die Installation, indem Sie erneut auf **Install** klicken.
Das Fenster **Installation Settings** bietet eine Übersicht über die Komponenten, die installiert werden. Vor dem Abschluss der Installation können Sie hier eventuell nötige Änderungen vornehmen.

Nachdem der Installationsvorgang abgeschlossen wurde, wird der Computer auf dem installierten System neu gestartet. Nehmen Sie die DVD aus dem DVD-Laufwerk.

Um eine geeignete Bildschirmauflösung zu wählen:

Installation des Linux-Servers

Konfiguration einer einheitlichen Zeitbasis

- Klicken Sie in der Taskleiste auf **Anwendungen**.
- Klicken Sie dann im Menübaum **Einstellungen > Displays**.
- Klicken Sie im Fenster **Displays** auf das Feld **Unbekanntes Display**
- Wählen Sie im Pop-up-Fenster **Unbekanntes Display** die entsprechende Auflösung aus der Aufklappliste **Auflösung** aus und klicken Sie dann auf **Übernehmen**.
- Klicken Sie abschließend im Bestätigungs-Pop-up-Fenster auf **Änderungen beibehalten**.

Nächste Schritte

NTP-Server konfigurieren (für eine einheitliche Zeitbasis).

8.6 Konfiguration einer einheitlichen Zeitbasis

Kommunikationssystem und IP-Teilnehmer (IP-Telefone, Client-PCs) sollten über eine einheitliche Zeitbasis (Datum und Uhrzeit) verfügen. Diese Zeitbasis wird von einem SNTP-Server zur Verfügung gestellt.

Als Zeitbasis sind folgende Varianten möglich:

- **SNTP-Server im internen Netz (empfohlen)**

Wenn möglich, sollte ein im internen Netz vorhandener SNTP-Server verwendet werden. In diesem Fall wird die IP-Adresse, die URL oder der DNS-Name des SNTP-Servers benötigt.

- **SNTP-Server im Internet**

Ist ein Internet-Zugang vorhanden und eingerichtet, kann auch ein SNTP-Server aus dem Internet verwendet werden. In diesem Fall wird die URL oder der DNS-Name des SNTP-Servers benötigt.

- **OpenScape Business X3/X5/X8 als SNTP-Server**

Alternativ kann das Kommunikationssystem OpenScape Business X3/X5/X8 als SNTP-Server verwendet werden. Voraussetzung ist, dass OpenScape Business X3/X5/X8 über ISDN-Leitungen mit dem Amt verbunden ist und die Systemzeit vom Amt übernommen wird. In diesem Fall ist zunächst OpenScape Business X3/X5/X8 für die Verwendung als SNTP-Server einzurichten (siehe Administratordokumentation) und anschließend ist die IP-Adresse von OpenScape Business X3/X5/X8 innerhalb von Linux als SNTP-Server einzutragen.

Die IP-Telefone erhalten Datum & Uhrzeit automatisch vom Softswitch OpenScape Business S oder bei OpenScape Business UC Booster Server vom Kommunikationssystem OpenScape Business X3/X5/X8. Die Client-PCs, auf denen die OpenScape Business Communications Clients installiert sind, müssen so eingestellt sein, dass sie zeitsynchron mit dem Softswitch OpenScape Business S bzw. dem Kommunikationssystem OpenScape Business X3/X5/X8 sind (siehe Anleitung des Betriebssystems der Client-PCs).

8.6.1 Wie Sie einen SNTP-Server konfigurieren

Schritt für Schritt

- 1) Klicken Sie in der Taskleiste auf **Anwendungen**.
- 2) Klicken Sie im Menübaum auf **Tools > YaST**.

- 3) Geben Sie das Passwort für den Benutzer root ein und klicken Sie auf **Continue**. Es öffnet sich das YaST2 Control Center.
- 4) Klicken Sie im Menübaum auf **System**.
- 5) Klicken Sie im Bereich **System** auf **Date and Time**.
- 6) Klicken Sie auf **Change**.
- 7) Aktivieren Sie die Option **Synchronize with NTP Server**.
- 8) Geben Sie einen NTP-Server ein:
 - **SNTP-Server im internen Netz** (empfohlen)
Geben Sie die IP-Adresse, die URL oder den DNS-Namen des SNTP-Servers direkt in das Listenfeld ein.
 - **SNTP-Server im Internet**
Wählen Sie den gewünschten SNTP-Server aus der Liste **NTP Server Address** aus oder geben Sie die URL oder den DNS-Namen des SNTP-Servers direkt in das Listenfeld ein.
 - **OpenScape Business X3/X5/X8 als SNTP-Server (nur bei OpenScape Business UC Booster Server)**
Geben Sie die IP-Adresse des Kommunikationssystems OpenScape Business X3/X5/X8 direkt in das Listenfeld ein.
- 9) Aktivieren Sie das Kontrollkästchen **Save NTP configuration**.
- 10) Klicken Sie auf **Configure**.
- 11) Aktivieren Sie die Option **Now and On Boot**.
- 12) Klicken Sie auf **OK** und anschließend auf **Accept**.
- 13) Schließen Sie das Fenster mit **OK**.
- 14) Schließen Sie das **YaST2Control Center**.

8.7 Updates

Um Updates zu erhalten, ist es nötig, sich direkt bei Novell zu registrieren.

Die Installation und der Betrieb der freigegebenen SLES 12 SP5 64 Bit Version ist ohne Registrierung möglich. Trotzdem ist es wichtig, sich bei Novell zu registrieren, um Sicherheits-Patches und Software-Updates zu erhalten.

Einen Novell Activation Code (Registrierungscode) können Sie über die Bestellposition "OpenScape Business SLES Upgrade key" beziehen. Bei der Bestellung erhalten Sie einen LAC (Lizenzaktivierungsschlüssel). Mit Hilfe dieses LAC können Sie sich am CLS (zentraler Lizenz-Server) den Activation Code herunterladen, mit dem Sie bei Novell ein Kundenkonto erstellen können. Es wird empfohlen, das Kundenkonto vor der Linux-Installation einzurichten.

Möglich sind folgende Update-Varianten: Die Registrierung bei Novell ist eine Voraussetzung.

- **Updates während der Linux-Installation (empfohlen)**

Während der Linux-Installation können Updates und Patches vom Novell-Download-Server online heruntergeladen werden.

Ausnahme: Service Packs dürfen nicht installiert werden.

- **Updates nach der Linux-Installation und vor der Installation der Kommunikationssoftware**

Nach der Linux-Installation können Updates und Patches vom Novell-Download-Server manuell über YaST (Software - Online-Updates) heruntergeladen werden.

Ausnahme: Service Packs dürfen nicht installiert werden.

- **Updates nach der Installation der Kommunikationssoftware**

Nach der Installation der Kommunikationssoftware können Updates und Patches vom Novell-Download-Server automatisch heruntergeladen werden. Dabei müssen Updates und Patches, die einen Neustart des Linux-Servers erfordern (interaktive Updates), übersprungen werden. Es wird empfohlen, nach ca. 2-3 Update-Prozessen ein manuelles Update zu starten, damit auch die übersprungenen, interaktiven Updates installiert werden.

Die entsprechenden Einstellungen sind über YaST (Software - Online-Updates) vorzunehmen.

Abweichungen von den zuvor genannten Varianten sind möglich und werden in der Release Note der Kommunikationssoftware beschrieben.

Anmerkung: Während eines SLES-Online-Updates fordert das Linux-Verwaltungstool Yast dazu auf, entweder rsyslog oder syslog-ng zu entfernen. Sie müssen nur das rsyslog-Paket entfernen, da das syslog-ng-Paket für die Tracing-Funktion von OpenScape Business S verwendet wird.

8.7.1 Wie Sie automatische Online-Updates aktivieren

Schritt für Schritt

- 1) Klicken Sie in der Taskleiste auf **Anwendungen**.
- 2) Klicken Sie im Menübaum auf **System-Tools > YaST**.
- 3) Geben Sie das Passwort für den Benutzer root ein und klicken Sie auf **Continue**. Das Fenster **Administratoreinstellungen** wird geöffnet.
- 4) Klicken Sie auf **Online Update Configuration**.
- 5) Aktivieren Sie das Kontrollkästchen **Automatic Online Update** und wählen Sie als Intervall **daily**, **weekly** or **monthly** aus.
- 6) Aktivieren Sie das Kontrollkästchen **Skip Interactive Patches**.
- 7) Klicken Sie auf **OK**.
- 8) Schließen Sie die **Administratoreinstellungen**.

8.7.2 Online-Updates manuell aktivieren

Schritt für Schritt

- 1) Klicken Sie in der Taskleiste auf **Anwendungen**.
- 2) Klicken Sie im Menübaum auf **System-Tools > YaST**.
- 3) Geben Sie das Passwort für den Benutzer root ein und klicken Sie auf **Continue**. Das Fenster **Administratoreinstellungen** wird geöffnet.

- 4) Klicken Sie auf **Online Update**. Es erscheint eine Aufstellung der verfügbaren, erforderlichen Patches (**Needed Patches**) im Bereich **Zusammenfassung**. Wenn Sie bereits alle aktuellen Patches installiert haben, ist diese Liste leer; andernfalls aktivieren Sie alle angezeigten Kontrollkästchen.
- 5) Klicken Sie auf **Accept**, um das manuelle Online-Update zu starten. Das Fenster schließt sich nach dem Update automatisch.
- 6) Schließen Sie die **Administratoreinstellungen**.

8.8 Sicherung und Wiederherstellung der Serversoftware

Es ist erforderlich das Linux-Betriebssystem zu sichern, damit es im Notfall wiederhergestellt werden kann.

Nach der Erstinbetriebnahme und vor jedem manuellen Update wird dringend empfohlen, mit einem geeigneten Tool eine vollständige Sicherung des Server-PCs bzw. der betroffenen Partitionen durchzuführen. Tritt z.B. nach einer Aktualisierung ein schwerwiegender Fehler auf, muss der Server-PC komplett wiederhergestellt werden.

In einer virtuellen Umgebung kann die gesamte virtuelle Maschine kopiert werden.

Wird der komplette Server-PC gesichert, sind die Daten der Kommunikationssoftware in dieser Sicherung enthalten. Wird nur das Betriebssystem gesichert, müssen zusätzlich auch die Daten der Kommunikationssoftware zyklisch gesichert werden.

9 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-Telefonienetz. 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
- Datensicherung

9.1 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-Telefonienetz) ist vorhanden und nutzbar.
- Die Hardware ist korrekt montiert und angeschlossen.
- Für die Integration 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 Erstinbetriebnahme 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 *Administratordokumentation*, *ErstInstallation X3/X5/X8*).
- Ein Rufnummernplan ist vorhanden und bekannt (siehe *Administratordokumentation - ErstInstallation X3/X5/X8*).

Admin-PC

Für den Administrations-PC (Admin-PC), mit dem die Erstinbetriebnahme 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.

9.2 Komponenten

Die Komponenten des Installationsbeispiels sind im Folgenden beschrieben und skizziert.

Das Installationsbeispiel umfasst folgende Komponenten:

Ersteinrichtung von OpenScape Business X

- 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.

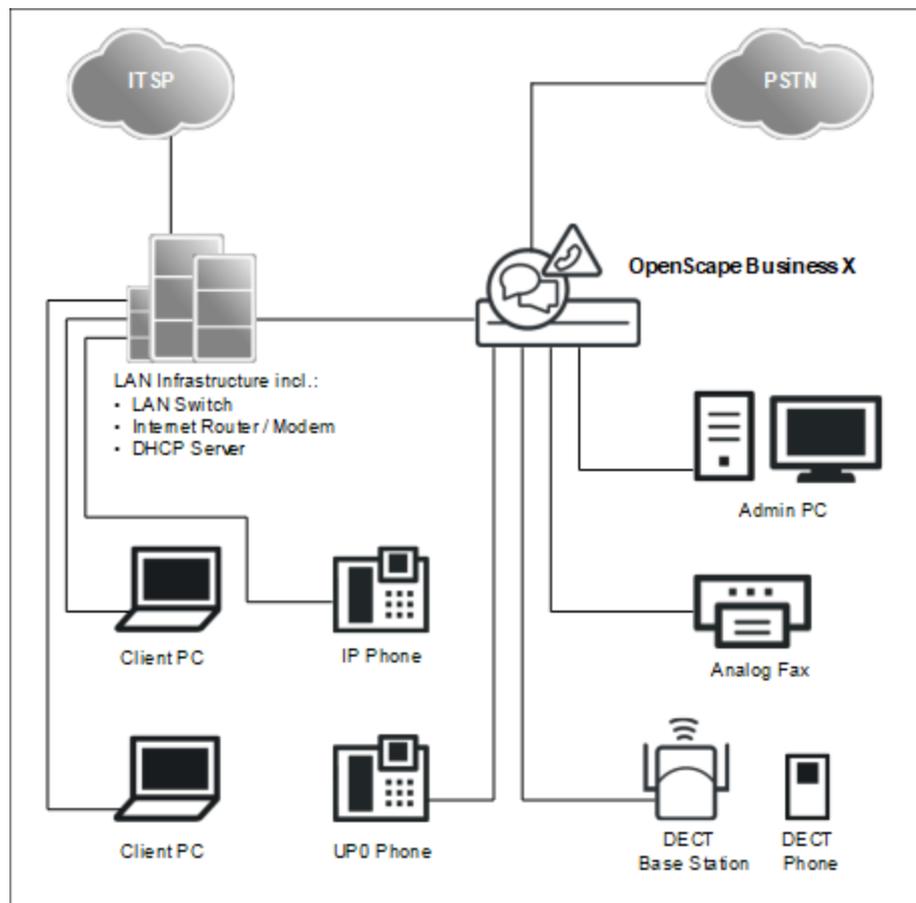
- Analoge Teilnehmer

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).



9.3 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
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.

9.4 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
192.168.1.50 bis 192.168.1.254	Client-PCs & IP-Telefone, zugleich IP-Adressband des DHCP-Servers, Zuweisung der IP-Adressen an die Clients erfolgt dynamisch

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

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

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

Erweiterung der Netzmaske bei Verwendung des voreingestellten Netzsegments

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

Voreingestellte Netzsegment-Konfiguration:

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

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

Beispiel einer geänderten Konfiguration:

- 192.168.1.2: IP-Adresse des Kommunikationssystems
- 255.255.0.0: Netzmaske
- 192.169.3.2: interne IP-Adresse des Kommunikationssystems

Änderbar über **Experten-Modus > Telefonie > Payload > HW-Module > DSP-Einstellungen ändern**

- 192.170.2.1: IP-Adresse der LAN3-Schnittstelle (Admin-Port)

Änderbar über **Experten-Modus > Telefonie > Netzwerkschnittstellen > Mainboard > LAN 3 (Admin)**

9.5 Erstinbetriebnahme

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

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

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



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



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



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

Anschluss des Admin-PCs

Um das Kommunikationssystem zu konfigurieren, wird der Admin-PC direkt an die LAN-Schnittstelle "LAN" des Kommunikationssystems angeschlossen

und so konfiguriert, dass er seine IP-Adresse vom internen DHCP-Server des Kommunikationssystems bezieht. Nach erfolgreicher Installation kann der Admin-PC ohne weitere Konfigurationsänderungen ins interne LAN integriert werden.

9.5.1 Wie Sie das Kommunikationssystem starten

Voraussetzungen

Die Montage der Hardware wurde ordnungsgemäß durchgeführt (siehe *OpenScape Business Installationsanleitung*).

Die Speicherkarte (mit der System-Software) ist gesteckt.

Das Kommunikationssystem ist noch nicht in das Kunden-LAN integriert.

Schritt für Schritt

Verbinden Sie das Kommunikationssystem mit dem Stromnetz.



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

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

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

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

9.5.2 Wie Sie den Admin-PC mit dem Kommunikationssystem verbinden

Voraussetzungen

Das Kommunikationssystem ist betriebsbereit.

Schritt für Schritt

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

Anmerkung: Die hier beschriebenen IP-Einstellungen gelten für Windows 7. Ausführliche Informationen zur

Einrichtung bei anderen Windows-Betriebssystemen entnehmen Sie bitte der jeweiligen Betriebssystemanleitung.

- a) Wählen Sie **Start > Systemsteuerung** und doppelklicken Sie auf **Netzwerk und Internet** und anschließend auf **Netzwerk- und Freigabecenter**.
 - b) Klicken Sie bei dem entsprechenden aktiven Netzwerk auf **LAN-Verbindung** und anschließend auf **Eigenschaften**.
 - c) Markieren Sie in der Registerkarte **Netzwerk** mit der linken Maustaste den Eintrag **Internetprotokoll Version 4 (TCP/IPv4)** und klicken Sie auf **Eigenschaften**.
 - d) Klicken Sie auf die Registerkarte **Allgemein** und kontrollieren Sie, ob das Optionsfeld **IP-Adresse automatisch beziehen** aktiviert ist. Falls nicht, aktivieren Sie es.
 - e) Schließen Sie alle geöffneten Fenster mit **OK**.
- 3) Verbinden Sie über ein LAN-Kabel die soeben konfigurierte LAN-Schnittstelle des Admin-PC mit der LAN-Schnittstelle "LAN" des Kommunikationssystems. Über diese Schnittstelle wird dem Admin-PC eine dynamische IP-Adresse zugewiesen.

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

9.5.3 Wie Sie das WBM starten

Voraussetzungen

Das Kommunikationssystem ist betriebsbereit. Die LED "Run" des Mainboards blinkt grün im 1Hz-Takt (0,5s an / 0,5s aus).

Admin-PC und Kommunikationssystem können über LAN miteinander kommunizieren.

Schritt für Schritt

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

`https://192.168.1.2`

Anmerkung: Lässt sich das WBM nicht starten, prüfen Sie die LAN-Verbindung und wiederholen Sie den Aufruf. Lässt es sich noch immer nicht starten, prüfen Sie, ob die IP-Adresse durch Ihre PC-interne Firewall geblockt wird. Genauere Informationen finden Sie in der Dokumentation Ihrer Firewall.

- 2) Wenn der Webbrowser ein Problem mit einem Sicherheitszertifikat meldet, installieren Sie das Zertifikat (am Beispiel der Internet Explorers V10).
 - a) Schließen Sie den Webbrowser.
 - b) Öffnen Sie den Webbrowser mit Administratorrechten, indem Sie mit der rechten Maustaste auf das Webbrowser-Symbol klicken und im Kontextmenü den Eintrag **Als Administrator ausführen** auswählen.
 - c) Erlauben Sie die Benutzerkontensteuerung.
 - d) Rufen Sie die Anmeldeseite von OpenScape Business Assistant (WBM) unter folgender Adresse auf:
`https://192.168.1.2`
 - e) Klicken Sie auf **Laden dieser Website fortsetzen**.
 - f) Klicken Sie auf die Meldung **Zertifikatsfehler** in der Navigationsleiste des Webbrowsers.
 - g) Klicken Sie auf **Zertifikate anzeigen**.
 - h) Klicken Sie auf **Zertifikat installieren** (nur sichtbar mit Administratorrechten).
 - i) Wählen Sie die Option **Lokaler Computer** und bestätigen Sie mit **Weiter**.
 - j) Wählen Sie die Option **Alle Zertifikate in folgendem Speicher speichern**, klicken Sie auf **Durchsuchen** und geben Sie **Vertrauenswürdige Stammzertifizierungsstellen** an.
 - k) Bestätigen Sie mit **OK** und anschließend mit **Weiter** und **Fertigstellen**.
 - l) Bestätigen Sie den Zertifikatimport mit **OK** und schließen Sie das Zertifikatsfenster mit **OK**.
 - m) Schließen Sie den Webbrowser.
 - n) Starten Sie den Webbrowser erneut (ohne Administratorrechte) und rufen Sie die Anmeldeseite von OpenScape Business Assistant (WBM) unter folgender Adresse auf:
`https://192.168.1.2`
- 3) Klicken Sie oben rechts auf das Sprachkürzel und wählen Sie aus dem Menü die Sprache aus, in der die Oberfläche des WBM angezeigt werden soll. Die Anmeldeseite wird in der ausgewählten Sprache angezeigt.
- 4) Geben Sie im ersten Feld unter **Login** den Standard-Benutzernamen `administrator@system` für den Zugang als Administrator ein.

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.

Nächste Schritte

Erstinstallation starten.

9.6 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.

9.6.1 Wie Sie den Wizard Erstinstallation starten

Voraussetzungen

Das WBM ist gestartet.

Schritt für Schritt

- 1) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
- 2) Klicken Sie auf **Bearbeiten**, um den Wizard **Erstinstallation** zu starten.

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

Nächste Schritte

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

9.6.2 Systemeinstellungen

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

Gehen Sie folgendermaßen vor:

1) Display-Logo und Produktbezeichnung festlegen

Sie können einen Display-Text festlegen, das im Display der Systemtelefone angezeigt wird. Zusätzlich können Sie die Produktbezeichnung auswählen.

2) IP-Adressen festlegen (falls nötig)

Dem Kommunikationssystem ist standardmäßig eine IP-Adresse und eine Subnetzmaske zugewiesen. Eventuell müssen Sie IP-Adresse und/oder Subnetzmaske an Ihren eigenen IP-Adressbereich anpassen.

Zusätzlich können Sie die IP-Adresse Ihres Default-Routers angeben, z.B. die IP-Adresse des Internet-Routers.

Das Application Board (UC Booster Card) benötigt ebenfalls eine IP-Adresse. Sie können unabhängig davon, ob es montiert ist oder nicht, eine IP-Adresse aus Ihrem IP-Adressbereich vergeben.

Soll die Netzmaske erweitert werden, z.B. von 255.255.255.0 auf 255.255.0.0, müssen sowohl die interne IP-Adresse des Kommunikationssystems als auch die IP-Adresse der LAN3-Schnittstelle (Admin-Port) geändert werden, da diese nicht im gleichen Netzsegment liegen dürfen wie die IP-Adresse der Kommunikationssystems (siehe auch [IP-Adressen-Schema](#) auf Seite 186).

9.6.2.1 Wie Sie das Display-Logo und die Produktbezeichnung festlegen

Voraussetzungen

Sie befinden sich im Fenster **Systemeinstellungen**.

The screenshot shows the 'System Settings' window in the 'Basic Installation - Initial Installation' wizard. It is divided into three sections: 'System Settings', 'OpenScope Business', and 'Application Board'. Each section contains input fields for IP addresses, netmasks, and default routing options.

Section	Field	Value
System Settings	Display Logo	OSBiz
	Brand	OpenScope Business
OpenScope Business	OpenScope Business - IP address	192.168.186.13
	OpenScope Business - Netmask	255.255.255.0
	OpenScope Business - Default Routing via	LAN
	OpenScope Business - IP Address of Default Router	192.168.186.22
Application Board	Application Board - IP address	192.168.1.3
	Application Board - Netmask	255.255.255.0
	Application Board - IP Address of Default Router	192.168.186.22

Schritt für Schritt

- 1) Geben Sie im Feld **Display-Logo** einen Text Ihrer Wahl ein (z.B. OpenScape Biz). Der Text kann bis zu 16 Zeichen lang sein. Vermeiden Sie Umlaute und Sonderzeichen.
- 2) Wählen Sie in der Aufklappliste **Produkt** die Produktbezeichnung aus.

Nächste Schritte

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

9.6.2.2 Wie Sie die IP-Adressen festlegen (optional)**Voraussetzungen**

Ihnen ist der IP-Adressbereich Ihres internen Netzes bekannt.

Sie befinden sich im Fenster **Systemeinstellungen**.

Schritt für Schritt

- 1) IP-Adresse des Kommunikationssystems festlegen:
 - a) Geben Sie im Feld **OpenScape Business - IP-Adresse** eine IP-Adresse ein, die im IP-Adressbereich Ihres internen Netzwerkes liegt (z. B. internes Netzwerk: 192.168.1.x, OpenScape Business: 192.168.1.2).

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

- b) Geben Sie im Feld **OpenScape Business - Netzmaske** die Netzmaske Ihres internen Netzwerkes an (z. B. 255.255.255.0).
- 2) IP-Adresse des Default-Routers festlegen:
 - a) Wählen Sie im Feld **OpenScape Business - Default Routing über** den Eintrag **LAN** aus.
 - b) Geben Sie im Feld **OpenScape Business - IP-Adresse des Default-Routers** die IP-Adresse Ihres Default-Routers an (z. B. internes

Ersteinrichtung von OpenScope Business X

Netzwerk: 192.168.1.x, Internet-Router als Default-Router:
192.168.1.1).

- 3) IP-Adresse der UC Booster Card festlegen (nötig, wenn gesteckt):
- 4) Klicken Sie auf **OK & Weiter**.

Nächste Schritte

DHCP konfigurieren.

9.6.2.3 So legen Sie Richtungsnamen fest

Voraussetzungen

Sie befinden sich im Fenster **Systemeinstellungen**.

System Settings

Display Logo:

Brand:

OpenScope Business

OpenScope Business - IP address:

OpenScope Business - Netmask:

OpenScope Business - Default Routing via:

OpenScope Business - IP Address of Default Router:

Application Board

Application Board - IP address:

Application Board - Netmask:

Application Board - IP Address of Default Router:

Schritt für Schritt

- 1) Aktivieren Sie das Kontrollkästchen **Automatische RSP.servicelink-Registrierung**:

Das Feld **Gerätename** kann bearbeitet werden.

- 2) Legen Sie **Gerätename** fest.

Wenn Sie die automatische RSP.servicelink-Registrierung auswählen, versucht das System alle 10 Minuten, sich automatisch zu registrieren und mit dem angegebenen Gerätenamen eine Verbindung zum RSP-Server herzustellen.

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

Nächste Schritte

DHCP konfigurieren.

9.6.3 DHCP-Einstellungen

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

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

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

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

Sie haben die folgenden 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 (*Administratordokumentation, Deployment Service (DLI und DLS)*).

- Internen DHCP-Server deaktivieren

Wird ein externer DHCP-Server genutzt, muss der interne DHCP-Server des Kommunikationssystems deaktiviert werden. Damit die IP-Systemtelefone automatisch mit der aktuellsten Telefonsoftware versorgt werden, müssen im externen DHCP-Server die netzwerkspezifischen Daten eingegeben werden, wie z.B. die IP-Adresse des internen DLI oder des externen DLS-Servers.

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.

9.6.3.1 Wie Sie den internen DHCP-Server deaktivieren

Voraussetzungen

Im internen Netz ist ein externer DHCP-Server (z.B. der DHCP-Server des Internet-Routers) aktiviert.

Sie befinden sich im Fenster **DHCP globale Einstellungen**.

Schritt für Schritt

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

Nächste Schritte

Länder- und Zeiteinstellungen konfigurieren.

9.6.3.2 Wie Sie den internen DHCP-Server aktivieren und konfigurieren

Voraussetzungen

Im internen Netz ist der externe DHCP-Server (z.B. der DHCP-Server des Internet-Routers) deaktiviert.

Sie befinden sich im Fenster **DHCP globale Einstellungen**.

Schritt für Schritt

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

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

Werden im internen Netz feste IP-Adressen verwendet (z.B. für einen Drucker-Server), muss der IP-Adressbereich (DHCP-Adress-Pool) so

gewählt werden, dass die festen IP-Adressen nicht innerhalb des IP-Adressbereichs liegen.

Beispiel:

Internet-Router: 192.168.1.1

OpenScape Business: 192.168.1.2

UC Booster Card: 192.168.1.3

Subnetz Adresse: 192.168.1.0

Netzmaske: 255.255.255.0

Drucker-Server: 192.168.1.10

DHCP-Adress-Pool: 192.168.1.50 bis 192.168.1.254

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

Nächste Schritte

Länder- und Zeiteinstellungen konfigurieren.

9.6.4 Länder- und Zeiteinstellungen

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

Gehen Sie folgendermaßen vor:

1) Länderkennzeichen und Sprache für Event-Logs auswählen

Für eine korrekte Länderinitialisierung müssen Sie das Land auswählen, in dem das Kommunikationssystem betrieben wird. Zusätzlich können Sie die Sprache auswählen, in der die Event-Logs (Protokolle für Systemereignisse, Fehler, usw.) abgespeichert werden.

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

Wenn Sie die integrierte Cordless-Lösung nutzen, geben Sie hier die systemweite DECT-Systemkennung ein.

3) Datum und Uhrzeit einstellen

- 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

Ersteinrichtung von OpenScope Business X

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).

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

Voraussetzungen

Sie befinden sich im Fenster **Basiskonfiguration**.

Setup - Wizards - Basic Installation - Initial Installation

Basic Configuration

Language settings

System Country Code: Germany

Language for Customer Trace Log: English

Time settings

Date and Time: Day: 03, Month: 03, Year: 2023, hh:mm:ss: 10:40:00

Timezone: (UTC +02:00) Athens, Beirut, Istanbul, Minsk

Detect date and time via an SNTP server

Date and Time via an external SNTP Server:

IP Address / DNS Name of External Time Server: 192.168.142.49

Poll Interval for External Time Server: Continuous

CMI data

System ID: 00000000

Schritt für Schritt

- 1) Wählen Sie in der Aufklappliste **System-Länderkennzeichen** das Land aus, in dem das Kommunikationssystem betrieben wird.
- 2) Wählen Sie im Feld **Sprache für Kunden-Eventlog** die Sprache aus, in der die Event-Logs (Protokolle für Systemereignisse, Fehler, usw.) ausgegeben werden sollen.

Nächste Schritte

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

oder

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

9.6.4.2 Wie Sie die DECT-Systemkennung eingeben

Voraussetzungen

Sie befinden sich im Fenster **Basiskonfiguration**.

Setup - Wizards - Basic Installation - Initial Installation

Basic Configuration

Language settings

System Country Code:

Language for Customer Trace Log:

Time settings

Date and Time: Day: Month: Year: hh:mm:ss:

Timezone:

Detect date and time via an SNTP server

Date and Time via an external SNTP Server:

IP Address / DNS Name of External Time Server:

Poll Interval for External Time Server:

CMI data

System ID:

Schritt für Schritt

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

Nächste Schritte

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

9.6.4.3 Wie Sie das Datum und die Uhrzeit manuell einstellen

Voraussetzungen

Sie befinden sich im Fenster **Basiskonfiguration**.

Setup - Wizards - Basic Installation - Initial Installation

Basic Configuration

Language settings

System Country Code:

Language for Customer Trace Log:

Time settings

Date and Time: Day: Month: Year: hh:mm:ss:

Timezone:

Detect date and time via an SNTP server

Date and Time via an external SNTP Server:

IP Address / DNS Name of External Time Server:

Poll Interval for External Time Server:

CMI data

System ID:

Schritt für Schritt

- 1) Geben Sie die aktuellen Werte für **Datum und Uhrzeit** ein.
- 2) Wählen Sie im Feld **Zeitzone** die gewünschte Zeitzone aus.

Ersteinrichtung von OpenScope Business X

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

Anmerkung: Wird die Zeitzoneneinstellung geändert, dann wird das System im letzten Schritt des Ersteinrichtungsassistenten **neu gestartet**.

Wenn die Zeitzoneneinstellung nicht geändert wird, wird das System nicht neu gestartet.

Nächste Schritte

UC-Lösung festlegen.

9.6.4.4 Wie Sie das Datum und die Uhrzeit von einem SNTP-Server beziehen

Voraussetzungen

Sie befinden sich im Fenster **Basiskonfiguration**.

Setup - Wizards - Basic Installation - Initial Installation

Basic Configuration

Language settings

System Country Code:

Language for Customer Trace Log:

Time settings

Date and Time: Day: Month: Year: hh:mm:ss:

Timezone:

Detect date and time via an SNTP server

Date and Time via an external SNTP Server:

IP Address / DNS Name of External Time Server:

Poll Interval for External Time Server:

CMI data

System ID:

Schritt für Schritt

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

Nächste Schritte

UC-Lösung festlegen.

9.6.5 UC-Lösung

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

Sie haben die folgenden Möglichkeiten:

- **Paket mit UC Smart**

Die UC-Lösung UC Smart ist auf dem OpenScape Business X Mainboard integriert.

- **Paket mit UC Suite**

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

- **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" integriert.

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

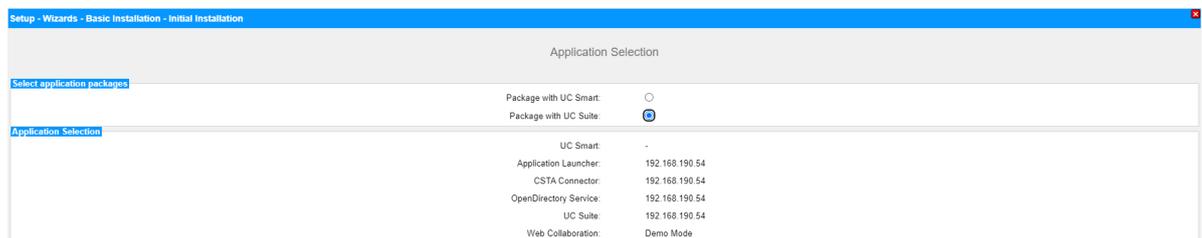
Die UC-Lösung UC Suite ist auf dem externen Linux-Server "OpenScape Business UC Booster Server" integriert.

9.6.5.1 Wie Sie die UC-Lösung festlegen

Voraussetzungen

Sie haben Lizenzen erworben entweder für die UC-Lösung UC Smart oder für die UC-Lösung UC Suite.

Sie befinden sich im Fenster **Applikationsauswahl ändern**.



Schritt für Schritt

- 1) Wenn Sie die UC-Lösung UC Smart ohne UC Booster Server nutzen, klicken Sie auf **Paket mit UC Smart**.
- 2) Wenn Sie die UC-Lösung UC Smart mit UC Booster Server nutzen, klicken Sie auf **Paket mit UC Smart auf OSBiz UC Booster-Server**. Geben Sie zusätzlich im Feld **IP-Adresse des OSBiz UC Booster-Servers** die IP-Adresse des externen Linux-Servers "OpenScape Business UC Booster Server" an.
- 3) Wenn Sie die UC-Lösung UC Suite mit UC Booster Card nutzen, klicken Sie auf **Paket mit UC Suite**.
- 4) Wenn Sie die UC-Lösung UC Suite mit UC Booster Server nutzen, klicken Sie auf **Paket mit UC Suite auf OSBiz UC Booster-Server**. Geben Sie zusätzlich im Feld **IP-Adresse des OSBiz UC Booster-Servers** die IP-Adresse des externen Linux-Servers "OpenScape Business UC Booster Server" an.
- 5) Klicken Sie auf **OK & Weiter**.
- 6) Der Wizard **Erstinstallation** ist abgeschlossen. Klicken Sie auf **Beenden**.

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

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

Nächste Schritte

Kommunikationssystem ans Kunden-LAN anschließen.

9.6.6 Anschluss des Kommunikationssystems ans Kunden-LAN

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

9.6.6.1 Wie Sie das Kommunikationssystem ans Kunden-LAN anschließen

Voraussetzungen

Das Kommunikationssystem ist betriebsbereit.

Schritt für Schritt

- 1) Entfernen Sie das LAN-Kabel des Admin-PC aus der mittleren LAN-Schnittstelle "LAN" und integrieren Sie den Admin-PC in das Kunden-LAN, indem Sie ihn z.B. an einen Switch anschließen.
- 2) Schließen Sie ein LAN-Kabel an die mittlere LAN-Schnittstelle "LAN" des Kommunikationssystems an.
- 3) Integrieren Sie das Kommunikationssystem über dieses LAN-Kabel in das Kunden-LAN, indem Sie es z.B. an einen Switch anschließen.
- 4) Ist eine UC Booster Card (Application Board) gesteckt, schließen Sie ein weiteres LAN-Kabel an die LAN-Schnittstelle "LAN2" der UC Booster Card an (rechte/untere der beiden LAN-Schnittstellen) und integrieren Sie die UC Booster Card über dieses LAN-Kabel in das Kunden-LAN, indem Sie es z.B. an einen Switch anschließen.

Nächste Schritte

Basiskonfiguration starten.

9.7 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.

9.7.1 Wie Sie den Wizard Basisinstallation starten

Voraussetzungen

Der Wizard **Erstinstallation** ist durchlaufen.

Das Kommunikationssystem ist ins Kunden-LAN integriert.

Das Kommunikationssystem ist betriebsbereit. Die LED "Run" des Mainboards blinkt grün im 1Hz-Takt (0,5s an / 0,5s aus).

Schritt für Schritt

- 1) Rufen Sie auf dem Admin-PC in Ihrem Webbrowser die Anmeldeseite des WBM unter folgender Adresse auf:
`https://<IP-Adresse von OpenScape Business>`
Die Standard-IP-Adresse von OpenScape Business ist 192.168.1.2, also z.B. `https://192.168.1.2`
- 2) Geben Sie im Feld **Benutzername** den Standard-Benutzernamen `administrator@system` für den Zugang als Administrator ein.
- 3) Geben Sie im Feld **Passwort** das von Ihnen während der Erstinbetriebnahme definierte Passwort ein.
- 4) Klicken Sie auf **Anmelden**.
- 5) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
- 6) Klicken Sie auf **Bearbeiten**, um den Wizard **Basisinstallation** zu starten.

Nächste Schritte

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

9.7.2 Systemrufnummern und Vernetzung

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

Gehen Sie folgendermaßen vor:

Ersteinrichtung von OpenScape Business X

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 Netzwerk eine eindeutige Knoten-ID besitzen.

9.7.2.1 Wie Sie die Systemrufnummern für einen Anlagenanschluss eingeben

Voraussetzungen

Sie haben einen Anlagenanschluss.

Sie befinden sich im Fenster **Systemüberblick**.

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:

Upstream of your internet connection

Upstream up to (Kbps):

Schritt für Schritt

- 1) Geben Sie im Feld **Ländervorwahl** die Ländervorwahl ein, z. B. 49 für Deutschland oder 1 für USA.
- 2) Geben Sie im Feld **Ortsnetzkenzahl** die Ortsvorwahl ein, z. B. 89 für München.

- 3) Geben Sie im Feld **Anlagenrufnummer** die Anlagenrufnummer Ihres Amtsanschlusses ein, z. B. 7007 (Ihre Anschlussnummer).
- 4) Ändern Sie das Feld **Internationales Präfix** nur wenn nötig. Für Deutschland gilt 00, für USA 011).

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

Nächste Schritte

Vernetzung aktivieren oder deaktivieren

9.7.2.2 Wie Sie die Systemrufnummern für einen Mehrgeräteanschluss eingeben

Voraussetzungen

Sie haben einen Mehrgeräteanschluss.

Sie befinden sich im Fenster **Systemüberblick**.

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:

Upstream of your internet connection

Upstream up to (Kbps):

Schritt für Schritt

- 1) Geben Sie im Feld **Ländervorwahl** die Ländervorwahl ein, z. B. 49 für Deutschland oder 1 für USA.
- 2) Geben Sie im Feld **Ortsnetzkenzahl** die Ortsvorwahl ein, z. B. 89 für München.
- 3) Lassen Sie das Feld **Anlagenrufnummer** leer.
- 4) Ändern Sie das Feld **Internationales Präfix** nur wenn nötig. Für Deutschland gilt 00, für USA 011).

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

Nächste Schritte

Vernetzung aktivieren oder deaktivieren

9.7.2.3 Wie Sie die Vernetzung aktivieren oder deaktivieren

Voraussetzungen

Sie befinden sich im Fenster **Systemüberblick**.

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 OpenScope Business in "OpenScope 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 OpenScope 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:

Upstream of your internet connection

Upstream up to (Kbps):

Schritt für Schritt

- 1) Wenn das Kommunikationssystem mit anderen Kommunikationssystemen vernetzt werden soll:
 - a) Aktivieren Sie das Kontrollkästchen **Netzwerk-Integration**.
 - b) Vergeben Sie im Feld **Knoten-ID** für das Kommunikationssystem eine im Netzwerk eindeutige Knoten-ID (Ziffern von 1 bis 100 möglich).
- 2) Wenn das Kommunikationssystem nicht mit anderen Kommunikationssystemen vernetzt werden soll, lassen Sie das Kontrollkästchen **Netzwerk-Integration** deaktiviert.

Nächste Schritte

Konfigurieren Sie den Upstream Ihrer Internetverbindung.

9.7.3 Teilnehmerdaten

Im Fenster **Zentrale Teilnehmer-Funktionen** können Sie bei Bedarf anstelle des vordefinierten Standardrufnummernplans Ihren individuellen Rufnummernplan konfigurieren und weitere Teilnehmerdaten importieren. Im Netzwerk muss der Standard-Rufnummernplan an den Rufnummernplan des Netzverbands 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 die folgenden 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: Wenn **Änderungen an vorkonfigurierten Funktionsrufnummern vorgenommen werden**, müssen in UC Suite durchgeführte benutzerdefinierte Konfigurationen überprüft oder erneut durchgeführt werden (z. B. Warteschlangen Pilotwarteschlangen)

- 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.

9.7.3.1 Wie Sie die Teilnehmerdaten anzeigen

Voraussetzungen

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

Schritt für Schritt

- 1) Aktivieren Sie das Optionsfeld **Teilnehmerkonfiguration anzeigen**.
- 2) Klicken Sie auf **Funktion ausführen**. Es wird Ihnen eine Liste der Teilnehmer mit den vorkonfigurierten Rufnummern (Standard-Rufnummernplan) angezeigt.
- 3) Klicken Sie auf **OK**. Sie werden zum Fenster **Zentrale Teilnehmer-Funktionen** zurückgeführt.
- 4) Wenn Sie keine Teilnehmerdaten ändern wollen, klicken Sie auf **OK & Weiter**.

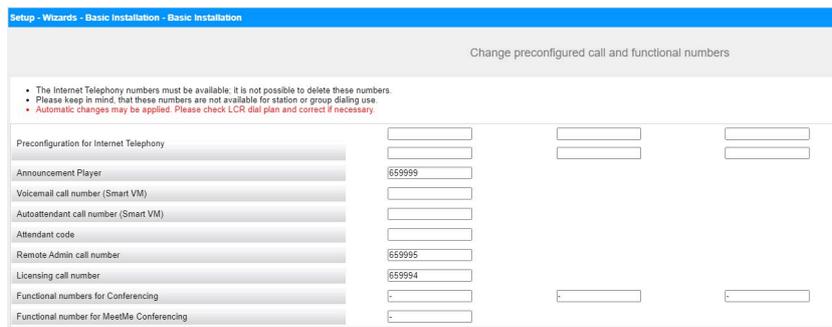
9.7.3.2 Wie Sie alle Rufnummern löschen

Voraussetzungen

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

Schritt für Schritt

- 1) Aktivieren Sie das Optionsfeld **Alle Rufnummern löschen**.
- 2) Aktivieren Sie das Kontrollkästchen **Alle Rufnummern löschen**.
- 3) Klicken Sie auf **Funktion ausführen**. Alle vorgelegten Rufnummern werden gelöscht. Anschließend erscheint das Fenster **Vorkonfigurierte Rufnummern ändern**.



- 4) Passen Sie die Kennzahlen und speziellen Rufnummern an Ihre Wünsche an und klicken Sie anschließend auf **OK**. Sie werden zum Fenster **Zentrale Teilnehmer-Funktionen** zurückgeführt.
- 5) Wenn Sie keine weiteren Teilnehmerdaten ändern wollen, klicken Sie auf **OK & Weiter**.

9.7.3.3 Wie Sie vorkonfigurierte Rufnummern an den individuellen Rufnummernplan anpassen

Voraussetzungen

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

Schritt für Schritt

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

- 3) Passen Sie die vorkonfigurierten Rufnummern an Ihre Wünsche an und klicken Sie anschließend auf **OK**. Sie werden zum Fenster **Zentrale Teilnehmer-Funktionen** zurückgeführt.
- 4) Wenn Sie keine weiteren Teilnehmerdaten ändern wollen, klicken Sie auf **OK & Weiter**.

9.7.3.4 Wie Sie die Teilnehmerdaten über eine XML-Datei importieren**Voraussetzungen**

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

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

Schritt für Schritt

- 1) Aktivieren Sie das Optionsfeld **XML-Datei mit Teilnehmerdaten importieren**.
- 2) Klicken Sie auf **Funktion ausführen**.
- 3) Wählen Sie mit **Durchsuchen** die erstellte XML-Datei aus und klicken Sie auf **Öffnen**.
- 4) Klicken Sie anschließend auf **OK**. Die Teilnehmerdaten werden importiert.
- 5) Klicken Sie auf **OK & Weiter**.

9.7.3.5 Anzeigen von Massendaten**Voraussetzungen**

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

Schritt für Schritt

- 1) Aktivieren Sie die Schaltfläche **Massendaten-Assistent**.
- 2) Klicken Sie auf **Funktion ausführen**.

- 3) Im Fenster **Massendaten-Assistent** können Sie die Einträge durch Klicken auf **Validieren** validieren. Es gibt zwei Arten der Validierung: den Front-End-Konsistenz Check und den Back-End-Konsistenz Check.
Ein grünes Validierungsfeld zeigt nur die Aktionen an, die kürzlich validiert wurden. Die Validierung der Daten wird nicht gespeichert. Wenn die Werte geändert werden, muss der Benutzer die Daten erneut validieren.
- 4) Während des Backend-Konsistenz-Checks und nach erfolgreicher Validierung der Daten ist keine Bearbeitung im Fenster **Massendaten-Assistent** möglich. Nach der erfolgreichen Validierung ist **OK&Weiter** im Bearbeitungsbeschränkungsmodus verfügbar. Wenn der Benutzer auf **Zurück** klickt, wird der Bearbeitungsmodus verfügbar, während **OK&Weiter** ausgeblendet wird. Schlägt die Validierung fehl, bleibt der Bearbeitungsmodus aktiv und **OK&Weiter** bleibt ausgeblendet.

Anmerkung: Der Benutzer kann auf **Zurück** klicken, um die Daten erneut zu bearbeiten, und das Fenster kehrt wieder in den Bearbeitungsmodus zurück. Der Bearbeitungsbeschränkungsmodus stellt sicher, dass der Benutzer nicht auf „OK&Weiter“ klicken und Änderungen übermitteln kann, die nicht validiert sind.

- 5) Klicken Sie nach der erfolgreichen Konfiguration von **Massendaten-Assistent** auf **Fertigstellen**. Auf der Seite „Fertigstellen“ wird eine Zusammenfassung mit allen Änderungen angezeigt.

Felder, die nicht bearbeitet werden können, sind bereits mit den relevanten Werten aus der Datenbank versehen. Als Folge davon wirkt sich die Funktion „Kopieren/Einfügen“ nicht auf die Daten aus.

Das Feld „Typ“ ist ein auswählbares Dropdown-Menü mit Bearbeitungsfunktion. Die einzigen zulässigen Optionen sind „No Port“, „System Client“, „SIP Client“, „Deskshare User“ und unter Umständen ein vordefinierter Wert, der auf der zugehörigen Baugruppe basiert. Wenn der Benutzer versucht, etwas anderes einzugeben, wird seine Eingabe verworfen, und das Dropdown-Menü wird nicht ausgeblendet, um eine ordnungsgemäße Eingabe zu gewährleisten.

Eine andere Einschränkung besteht darin, dass einige Ports nicht änderbar sind (z. B. ist für Ports, die zu einer analogen Karte gehören, der Typ nicht änderbar und „Analoger Teilnehmer“ bleiben). Es gelten alle Einschränkungen, wenn der Benutzer versucht, Text in die Spalte „Typ“ zu kopieren. Wenn der Benutzer versucht, irrelevante Daten einzufügen, ohne die obigen Regeln zu verletzen, kann „Kopieren und Einfügen“ überhaupt nicht ausgeführt werden.

„Kopieren und Einfügen“ kann sowohl auf die gesamte Tabelle als auch auf bestimmte Teile angewendet werden.

Anmerkung: Wenn Sie zwei aufeinanderfolgende Zellen mit einem numerischen Wert auswählen und die Felder nach unten ziehen, werden die folgenden Spalten nicht mit aufsteigenden Zahlen versehen, sondern mit einer Kopie der Werte aus den ausgewählten Zellen.

9.7.4 ISDN-Konfiguration

Im Fenster **ISDN-Konfiguration** legen Sie fest, ob ISDN-Teilnehmer angeschlossen werden sollen und ob der Amtsanschluss über ISDN erfolgen soll. Der ISDN-Amtsanschluss kann als ISDN-Anlagenanschluss und/oder ISDN-Mehrgeräteanschluss eingerichtet werden. Je nach Kommunikationssystem und evtl. verwendeter Baugruppe stehen dafür unterschiedlich viele S₀-Schnittstellen zur Verfügung.

Sie haben die folgenden 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.

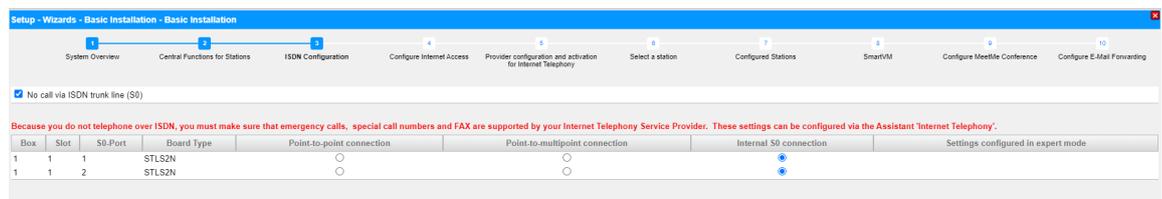
Weitere Möglichkeiten für einen Amtsanschluss

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.

9.7.4.1 Wie Sie den Anschluss von ISDN-Teilnehmern konfigurieren

Voraussetzungen

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



Ersteinrichtung von OpenScape Business X

Schritt für Schritt

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

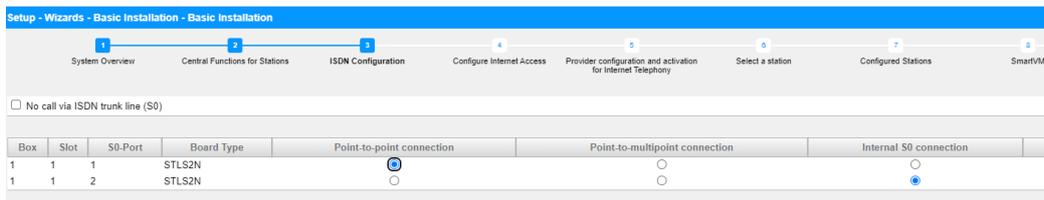
Nächste Schritte

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

9.7.4.2 Wie Sie den ISDN-Anlagenanschluss konfigurieren

Voraussetzungen

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



Schritt für Schritt

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

9.7.4.3 Wie Sie den ISDN-Mehrgeräteanschluss konfigurieren

Voraussetzungen

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



Schritt für Schritt

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

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

Box	Slot	S0-Port	ISDN Multiple Subscriber Numbers
1	1	1	
1	1	2	
1	1	3	
1	1	4	
1	1	5	
1	1	6	
1	1	7	
1	1	8	
1	1	9	
1	1	10	

4) Geben Sie in der Spalte **ISDN-Mehrfachrufnummern** alle Rufnummern (MSN) ein, die Ihnen Ihr Netzanbieter mitgeteilt hat. Pro S₀-Anschluss können Sie bis zu 10 MSN eingeben. Die Anzahl der S₀-Anschlüsse ist abhängig vom Kommunikationssystem und von der evtl. verwendeten Baugruppe.

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

9.7.4.4 Wie Sie die ISDN-Konfiguration deaktivieren

Voraussetzungen

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

Schritt für Schritt

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

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

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

9.7.5 Internet-Zugang

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

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

Von den hier aufgeführten Möglichkeiten ist nur eine auszuwählen.

- Internet-Zugang über ein Internet-Modem (**DSL am WAN Port direkt**)

Sie wollen das Kommunikationssystem direkt an einem Internet-Modem (DSL, Kabel, UMTS ...) betreiben. OpenScape Business hat den Internet-

Router integriert. Geben Sie die Zugangsdaten des Internet-Service-Providers (ISP) direkt im Kommunikationssystem ein und nutzen den WAN-Anschluss des Kommunikationssystems.



Sie haben die folgenden 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.

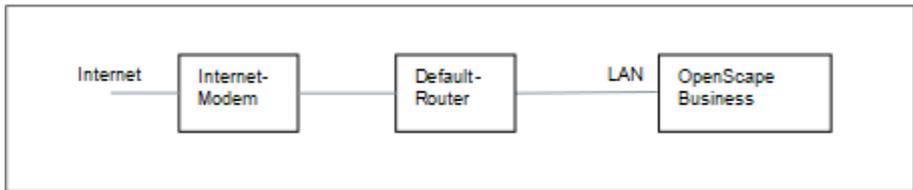
Sie haben die folgenden Möglichkeiten:

- **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.

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

Voraussetzungen

Das Kommunikationssystem muss über die LAN-Schnittstelle "LAN" mit dem Kunden-LAN verbunden sein. Die Verbindung darf nicht über den WAN-Anschluss erfolgen, da dieser deaktiviert wird.

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

Schritt für Schritt

- 1) Deaktivieren Sie das Kontrollkästchen **Kein Internet-Zugang**.
- 2) Aktivieren Sie das Optionsfeld **TCP/IP am LAN Port über einen externen Router**, geben Sie im Feld **Upstream bis zu (Kbit/s)** den Wert für die Upload-Geschwindigkeit Ihrer Internet-Verbindung ein und klicken Sie auf **OK & Weiter**.

- 3) Geben Sie im Feld **IP-Adresse des bevorzugten DNS-Servers** die IP-Adresse des lokalen DNS-Servers (z.B. Internet-Router) oder des Internet-DNS-Servers (z.B. für Internet-Telefonie) ein.
- 4) Geben Sie im Feld **IP-Adresse des Default Routers** die IP-Adresse des externen Internet-Routers ein.
- 5) Klicken Sie auf **OK & Weiter**.

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

Voraussetzungen

Das Kommunikationssystem muss über die LAN-Schnittstelle "WAN" mit dem LAN-Segment des Kunden-LAN verbunden sein, indem sich der Internet-Router befindet.

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

Schritt für Schritt

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

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

The screenshot shows the 'Internet Access' configuration window in the OpenScope Business X installation wizard. The window title is 'Setup - Wizards - Basic Installation - Basic Installation'. The progress bar at the top indicates the current step is 'Internet Access'. The configuration options are as follows:

- Automatic Address Configuration (via DHCP):
- IP Address:
- Subnet Mask:
- MAC Address:
- Ethernet Link Mode:
- Max. Data Packet Size (bytes):
- Network Address Translation:
- Bandwidth Control for Voice Connections:
- Bandwidth for Downloads:
- Bandwidth for Uploads:
- Bandwidth Used for Voice/Fax (%):
- IEEE802.1p/q Tagging:
- IEEE802.1p/q VLAN ID:

- 3) Wenn für die WAN-Schnittstelle die netzwerkspezifischen Daten von einem bereits aktiven DHCP-Server bezogen werden sollen:
 - a) Aktivieren Sie das Kontrollkästchen **Automatische Adresskonfiguration (mit DHCP)**.
 - b) Aktivieren Sie das Kontrollkästchen **IP-Adresse des Default Routers übernehmen**.
 - c) Aktivieren Sie bei Bedarf das Kontrollkästchen **IP-Adresse des DNS-Servers übernehmen**.
 - d) Aktivieren Sie bei Bedarf das Kontrollkästchen **IP-Adresse des SNTP-Servers übernehmen**.
- 4) Wenn der WAN-Schnittstelle eine feste IP-Adresse zugeordnet werden soll:
 - a) Deaktivieren Sie das Kontrollkästchen **Automatische Adresskonfiguration (mit DHCP)**.
 - b) Geben Sie die gewünschte **IP-Adresse** und **Netzmaske** der WAN-Schnittstelle ein.
- 5) Aktivieren Sie das Kontrollkästchen **Netzwerkadressübersetzung (NAT)**.
- 6) Wenn Sie zusätzlich Internet-Telefonie nutzen wollen, wählen Sie aus der Aufklappliste **Bandbreitensteuerung für Sprach-Verbindungen** den Eintrag **Nur Upload** oder **Upload und Download** je nach Bedarf aus. Bei einer hohen Download-Bandbreite und zugleich niedrigen Upload-Bandbreite sollte die Bandbreitensteuerung nur für den Upload aktiviert werden, damit nicht unnötig viel Download-Bandbreite für die Sprachübertragung reserviert wird.
- 7) Geben Sie in den Feldern **Bandbreite Download** und **Bandbreite Upload** die Bandbreite in kbit/s für den Download und Upload ein, die Ihnen Ihr Internet-Service-Provider zur Verfügung stellt.
- 8) Klicken Sie auf **OK & Weiter**.

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

Voraussetzungen

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

Die Internet-Zugangsdaten Ihres ISP liegen Ihnen vor (z.B. Benutzerkennung, Passwort, Bandbreite für Upload und Download).

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

Schritt für Schritt

- 1) Deaktivieren Sie das Kontrollkästchen **Kein Internet-Zugang**.
- 2) Aktivieren Sie das Optionsfeld **DSL am WAN Port des Mainboard direkt** und klicken Sie auf **OK & Weiter**.

- 3) Wählen Sie aus der Aufklappliste **Internet-Service-Provider-Auswahl** Ihren ISP aus.
- 4) Geben Sie im Bereich **Internet-Zugangsdaten für...** die Zugangsdaten ein, die Sie von ihrem ISP bekommen haben. Die Felder in diesem Bereich sind providerabhängig. Achten Sie bei der Eingabe der Daten auf korrekte Groß- und Kleinschreibung.
- 5) Wählen Sie im Bereich **Router-Einstellungen** unter **Dauerverbindung** abhängig von Ihrem Tarifmodell eine der beiden folgenden Optionen aus:
 - Haben Sie als Tarifmodell eine Flatrate, aktivieren Sie das Optionsfeld **An**. Legen Sie im Feld **Zwangstrennung um (Std:Min)** die Uhrzeit fest, zu der die Internet-Verbindung getrennt werden soll (z.B. 01:30). Zu dieser Zeit sollten keine Daten mit dem Internet ausgetauscht werden (z.B. Software-Downloads oder Internet-Telefonie).
 - Haben Sie als Tarifmodell einen Zeittarif, aktivieren Sie das Optionsfeld **Aus**. Geben Sie im Feld **Automatisch trennen nach (Sekunden)** die Zeitdauer der Inaktivität an, nach der die Verbindung getrennt werden soll (z.B. 60 Sekunden).
- 6) Stellen Sie im Bereich **QoS-Parameter** die folgenden Werte ein:
 - a) Geben Sie in den Feldern **Bandbreite Download** und **Bandbreite Upload** die Bandbreite in kbit/s für den Download bzw. Upload ein, die Ihnen Ihr ISP zur Verfügung stellt.
 - b) Wenn Sie zusätzlich Internet-Telefonie nutzen wollen, wählen Sie aus der Aufklappliste **Bandbreitensteuerung für Sprach-Verbindungen** den Eintrag **Nur Upload** oder **Upload und Download** je nach Bedarf aus. Geben Sie im Feld **Bandbreite für Sprach-/Fax-Verbindungen (%)** in Prozent an, wieviel Bandbreite für Sprach- und Fax-Verbindungen reserviert werden soll (Standardwert: 80%).
- 7) Klicken Sie auf **OK & Weiter**. Sie werden zum Fenster **DynDNS-Account einrichten** geführt.
- 8) Wenn Sie VPN oder den Remote-Zugang nutzen wollen und keine öffentliche statische IP-Adresse haben, müssen Sie einen DynDNS-Account beantragt haben (z.B. bei dyndns.org) und ihn einrichten.
 - a) Wenn Ihr gewünschter DynDNS-Anbieter in der Aufklappliste **Domainname** enthalten ist, wählen Sie ihn aus der Liste aus (z.B. dyndns.org).
 - b) Wenn Ihr gewünschter DynDNS-Anbieter nicht in der Aufklappliste **Domainname** enthalten ist, aktivieren Sie das Kontrollkästchen

Benutzerdefinierte Domäne. Geben Sie im Feld **Domainname** den gewünschten DynDNS-Anbieter ein und in dem Feld **Update-URL** die Update-URL des DynDNS-Anbieters. Der Aufbau dieser URL ist abhängig vom DynDNS-Anbieter. Zusätzlich sind kundenspezifische Parameter (im Beispiel *kursiv* markiert) zu ergänzen.

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

- c) Geben Sie **Benutzername** und **Passwort** Ihres DynDNS-Accounts ein.
- d) Geben Sie im Feld **Hostname** Ihren vom DynDNS-Anbieter zugeteilten Hostnamen ohne den Domännennamen ein, z.B. myhost. Ihr vollständiger Domännennamen lautet dann z.B. myhost.dyndns.org.
- e) Testen Sie den DynDNS-Account mit **Verbindung testen**.
- f) Klicken Sie nach erfolgreichem Test auf **OK**.
- g) Klicken Sie auf **OK & Weiter**.
- 9) Wenn Sie eine öffentliche statische IP-Adresse haben oder VPN oder den Remote-Zugang nicht nutzen wollen, klicken Sie auf **kein DynDNS**.
- 10) Klicken Sie auf **OK & Weiter**.

9.7.5.4 Internet-Zugang über Standard-ISP PPPoE konfigurieren

Voraussetzungen

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

Folgende Internet-Zugangsdaten Ihres ISP liegen Ihnen vor:

Feldname	Beschreibung	Wert vom ISP
IP-Parameter (nur bei fester IP-Adresse)		
Partner-IP-Adresse der PPP-Verbindung	IP-Adresse des Servers Ihres ISP.	
Lokale IP-Adresse der PPP-Verbindung	IP-Adresse, die Ihnen vom ISP für den Internet-Zugang zugeteilt wurde.	
Authentifizierung (über PAP oder CHAP). PAP wird kaum noch verwendet, da die Authentifizierung unverschlüsselt ist.		
PPP-Benutzername	Benutzername für die PPP-Verbindung, der Ihnen vom ISP zugeteilt wurde.	
PAP-Authentifizierungsmodus	Authentifizierungsmodus für die PPP-Verbindung über PAP: PAP-Client , PAP-Host oder nicht benutzt .	
PAP-Kennwort	Kennwort für Authentifizierung durch PAP, das Ihnen vom ISP zugeteilt wurde.	
CHAP-Authentifizierungsmodus	Authentifizierungsmodus für die PPP-Verbindung über CHAP: CHAP-Client , CHAP-Host , CHAP-Client und -Host oder nicht benutzt .	

Feldname	Beschreibung	Wert vom ISP
CHAP-Kennwort	Kennwort für Authentifizierung durch CHAP, das Ihnen vom ISP zugeteilt wurde.	
QoS-Parameter der Schnittstelle		
Bandbreite Download	Wert der gesamten Bandbreite in kbit/s für den Download vom ISP.	
Bandbreite Upload	Wert der gesamten Bandbreite in kbit/s für den Upload zum ISP.	

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

Schritt für Schritt

- 1) Deaktivieren Sie das Kontrollkästchen **Kein Internet-Zugang**.
- 2) Aktivieren Sie das Optionsfeld **DSL am WAN Port direkt** und klicken Sie auf **OK & Weiter**.
- 3) Wählen Sie aus der Aufklappliste **Internet-Service-Provider-Auswahl** den Standard ISP Typ **Provider-PPPoE** aus.
- 4) Aktivieren Sie im Bereich **IP-Parameter** das Kontrollkästchen **IP-Parameter** nur, wenn vom ISP eine Anpassung gefordert wird. Geben Sie in diesem Fall in den Feldern **Partner-IP-Adresse der PPP-Verbindung**, **Lokale IP-Adresse der PPP-Verbindung** und **Max. Datenpaketlänge (Byte)** die Werte ein, die Sie von Ihrem ISP bekommen haben. Wählen Sie aus der Aufklappliste **IP-Address-Aushandlung** den Eintrag **konfigurierte IP-Adresse nutzen** aus.
- 5) Wählen Sie im Bereich **Router-Einstellungen** unter **Dauerverbindung** abhängig von Ihrem Tarifmodell eine der beiden folgenden Optionen aus:
 - Haben Sie als Tarifmodell eine Flatrate, aktivieren Sie das Optionsfeld **An**. Legen Sie im Feld **Zwangstrennung um (Std:Min)** die Uhrzeit fest, zu der die Internet-Verbindung getrennt werden soll (z.B. 01:30). Zu dieser Zeit sollten keine Daten mit dem Internet ausgetauscht werden (z.B. Software-Downloads oder Internet-Telefonie).
 - Haben Sie als Tarifmodell einen Zeittarif, aktivieren Sie das Optionsfeld **Aus**. Geben Sie im Feld **Automatisch trennen nach (Sekunden)** die Zeitdauer der Inaktivität an, nach der die Verbindung getrennt werden soll (z.B. 60 Sekunden).
- 6) Die Einstellungen im Bereich **Authentifizierung** hängen davon ab, ob der ISP eine Authentifizierung über PPP fordert oder nicht.
 - Authentifizierung wird vom ISP gefordert: Stellen Sie sicher, dass das Kontrollkästchen **PPP-Authentifizierung** aktiviert ist. Geben Sie als PPP-Benutzernamen den Internet-Zugangsnamen des ISP an. Der gebräuchliche Standard ist der Authentifizierungsmodus **CHAP-Client**.
 - Authentifizierung wird vom ISP nicht gefordert: Stellen Sie sicher, dass das Kontrollkästchen **PPP-Authentifizierung** deaktiviert ist.
- 7) Wenn Sie NAT nutzen wollen, aktivieren Sie im Bereich **Adressenübersetzung** das Kontrollkästchen **NAT** (standardmäßig aktiviert).

- 8) Stellen Sie im Bereich **QoS-Parameter der Schnittstelle** die folgenden Werte ein:
 - a) Geben Sie in den Feldern **Bandbreite Download** und **Bandbreite Upload** die Bandbreite in kbit/s für den Download bzw. Upload ein, die Ihnen Ihr ISP zur Verfügung stellt.
 - b) Wenn Sie zusätzlich Internet-Telefonie nutzen wollen, wählen Sie aus der Aufklappliste **Bandbreitensteuerung für Sprach-Verbindungen** den Eintrag **Nur Upload** oder **Upload und Download** je nach Bedarf aus. Geben Sie im Feld **Bandbreite für Sprach-/Fax-Verbindungen (%)** in Prozent an, wieviel Bandbreite für Sprach- und Fax-Verbindungen reserviert werden soll (Standardwert: 80%).
- 9) Klicken Sie auf **OK & Weiter**. Sie werden zum Fenster **DynDNS-Account einrichten** geführt.
- 10) Wenn Sie VPN oder den Remote-Zugang nutzen wollen und keine öffentliche statische IP-Adresse haben, müssen Sie einen DynDNS-Account beantragt haben (z.B. bei dyndns.org) und ihn einrichten.
 - a) Wenn Ihr gewünschter DynDNS-Anbieter in der Aufklappliste **Domainname** enthalten ist, wählen Sie ihn aus der Liste aus (z.B. dyndns.org).
 - b) Wenn Ihr gewünschter DynDNS-Anbieter nicht in der Aufklappliste **Domainname** enthalten ist, aktivieren Sie das Kontrollkästchen **Benutzerdefinierte Domäne**. Geben Sie im Feld **Domainname** den gewünschten DynDNS-Anbieter ein und in dem Feld **Update-URL** die Update-URL des DynDNS-Anbieters. Der Aufbau dieser URL ist abhängig vom DynDNS-Anbieter. Zusätzlich sind kundenspezifische Parameter (im Beispiel *kursiv* markiert) zu ergänzen.


```
http://www.anydns.info/update.php?
user=<username>&password=<pass>&host=<domain>&ip=<ipaddr>
```
 - c) Geben Sie **Benutzername** und **Passwort** Ihres DynDNS-Accounts ein.
 - d) Geben Sie im Feld **Hostname** Ihren vom DynDNS-Anbieter zugeteilten Hostnamen ohne den Domänennamen ein, z. B. myhost. Ihr vollständiger Domänename lautet dann z.B. myhost.dyndns.org.
 - e) Testen Sie den DynDNS-Account mit **Verbindung testen**.
 - f) Klicken Sie nach erfolgreichem Test auf **OK**.
 - g) Klicken Sie auf **OK & Weiter**.
- 11) Wenn Sie eine öffentliche statische IP-Adresse haben oder VPN oder den Remote-Zugang nicht nutzen wollen, klicken Sie auf **kein DynDNS**.
- 12) Klicken Sie auf **OK & Weiter**.

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

Voraussetzungen

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

Folgende Internet-Zugangsdaten Ihres ISP liegen Ihnen vor:

Feldname	Beschreibung	Wert vom ISP
IP-Parameter (nur bei fester IP-Adresse)		
Partner-IP-Adresse der PPP-Verbindung	IP-Adresse des Servers Ihres ISP.	

Feldname	Beschreibung	Wert vom ISP
Lokale IP-Adresse der PPP-Verbindung	IP-Adresse, die Ihnen vom ISP für den Internet-Zugang zugeteilt wurde.	
PPTP-Parameter		
Lokale IP-Adresse der Kontrollverbindung	IP-Adresse, die Ihnen vom ISP für die PPTP-Verbindung zugeteilt wurde. Der voreingestellte Wert lautet 10.0.0.140.	
Partner-IP-Adresse der Kontrollverbindung	IP-Adresse des ISP-Servers für die PPTP-Verbindung. Der voreingestellte Wert lautet 10.0.0.138.	
Partner-Netzmaske für die Kontrollverbindung	Netzmaske, die Ihnen vom ISP für die PPTP-Verbindung zugeteilt wurde. Der voreingestellte Wert lautet 255.255.255.248.	
Authentifizierung (über PAP oder CHAP). PAP wird kaum noch verwendet, da die Authentifizierung unverschlüsselt ist.		
PPP-Benutzername	Benutzername für die PPP-Verbindung, der Ihnen vom ISP zugeteilt wurde.	
PAP-Authentifizierungsmodus	Authentifizierungsmodus für die PPP-Verbindung über PAP: PAP-Client , PAP-Host oder nicht benutzt .	
PAP-Kennwort	Kennwort für Authentifizierung durch PAP, das Ihnen vom ISP zugeteilt wurde.	
CHAP-Authentifizierungsmodus	Authentifizierungsmodus für die PPP-Verbindung über CHAP: CHAP-Client , CHAP-Host , CHAP-Client und -Host oder nicht benutzt .	
CHAP-Kennwort	Kennwort für Authentifizierung durch CHAP, das Ihnen vom ISP zugeteilt wurde.	
QoS-Parameter der Schnittstelle		
Bandbreite Download	Wert der gesamten Bandbreite in kbit/s für den Download vom ISP.	
Bandbreite Upload	Wert der gesamten Bandbreite in kbit/s für den Upload zum ISP.	

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

Schritt für Schritt

- 1) Deaktivieren Sie das Kontrollkästchen **Kein Internet-Zugang**.
- 2) Aktivieren Sie das Optionsfeld **DSL am WAN Port direkt** und klicken Sie auf **OK & Weiter**.

- 3) Wählen Sie aus der Aufklappliste **Internet-Service-Provider-Auswahl** den Standard ISP Typ **Provider-PPTP** aus.
- 4) Aktivieren Sie im Bereich **IP-Parameter** das Kontrollkästchen **IP-Parameter** nur, wenn vom ISP eine Anpassung gefordert wird. Geben Sie in diesem Fall in den Feldern **Partner-IP-Adresse der PPP-Verbindung**, **Lokale IP-Adresse der PPP-Verbindung** und **Max. Datenpaketlänge (Byte)** die Werte ein, die Sie von Ihrem ISP bekommen haben. Wählen Sie aus der Aufklappliste **IP-Address-Aushandlung** den Eintrag **konfigurierte IP-Adresse nutzen** aus.
- 5) Geben Sie in dem Bereich **PPTP-Parameter** die Werte ein, die Sie von Ihrem ISP bekommen haben.
- 6) Wenn Sie als Tarifmodell einen Zeittarif haben, aktivieren Sie das Kontrollkästchen **Short-Hold-Modus**. Geben Sie im Feld **Short-Hold-Zeit (s)** die Zeitdauer der Inaktivität an, nach der die Verbindung getrennt werden soll (z.B. 60 Sekunden).
- 7) Die Einstellungen im Bereich **Authentifizierung** hängen davon ab, ob der ISP eine Authentifizierung über PPP fordert oder nicht.
 - Authentifizierung wird vom ISP gefordert: Stellen Sie sicher, dass das Kontrollkästchen **PPP-Authentifizierung** aktiviert ist. Geben Sie als PPP-Benutzernamen den Internet-Zugangsnamen des ISP an. Treffen Sie die PAP- und CHAP-Einstellungen, wie Sie sie von Ihrem ISP zugeteilt bekommen haben.
 - Authentifizierung wird vom ISP nicht gefordert: Stellen Sie sicher, dass das Kontrollkästchen **PPP-Authentifizierung** deaktiviert ist.
- 8) Wenn Sie NAT nutzen wollen, aktivieren Sie im Bereich **Adressenübersetzung** das Kontrollkästchen **NAT** (standardmäßig aktiviert).
- 9) Stellen Sie im Bereich **QoS-Parameter der Schnittstelle** die folgenden Werte ein:
 - a) Geben Sie in den Feldern **Bandbreite Download** und **Bandbreite Upload** die Bandbreite in kbit/s für den Download bzw. Upload ein, die Ihnen Ihr ISP zur Verfügung stellt.
 - b) Wenn Sie zusätzlich Internet-Telefonie nutzen wollen, wählen Sie aus der Aufklappliste **Bandbreitensteuerung für Sprach-Verbindungen** den Eintrag **Nur Upload** oder **Upload und Download** je nach Bedarf aus. Geben Sie im Feld **Bandbreite für Sprach-/Fax-Verbindungen (%)** in Prozent an, wieviel Bandbreite für Sprach- und Fax-Verbindungen reserviert werden soll (Standardwert: 80%).
- 10) Klicken Sie auf **OK & Weiter**. Sie werden zum Fenster **DynDNS-Account einrichten** geführt.
- 11) Wenn Sie VPN oder den Remote-Zugang nutzen wollen und keine öffentliche statische IP-Adresse haben, müssen Sie einen DynDNS-Account beantragt haben (z.B. bei dyndns.org) und ihn einrichten.
 - a) Wenn Ihr gewünschter DynDNS-Anbieter in der Aufklappliste **Domainname** enthalten ist, wählen Sie ihn aus der Liste aus (z.B. dyndns.org).
 - b) Wenn Ihr gewünschter DynDNS-Anbieter nicht in der Aufklappliste **Domainname** enthalten ist, aktivieren Sie das Kontrollkästchen **Benutzerdefinierte Domäne**. Geben Sie im Feld **Domainname** den gewünschten DynDNS-Anbieter ein und in dem Feld **Update-URL** die Update-URL des DynDNS-Anbieters. Der Aufbau dieser URL ist

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

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

- c) Geben Sie **Benutzername** und **Passwort** Ihres DynDNS-Accounts ein.
 - d) Geben Sie im Feld **Hostname** Ihren vom DynDNS-Anbieter zugeteilten Hostnamen ohne den Domännennamen ein, z. B. myhost. Ihr vollständiger Domännennamen lautet dann z.B. myhost.dyndns.org.
 - e) Testen Sie den DynDNS-Account mit **Verbindung testen**.
 - f) Klicken Sie nach erfolgreichem Test auf **OK**.
 - g) Klicken Sie auf **OK & Weiter**.
- 12) Wenn Sie eine öffentliche statische IP-Adresse haben oder VPN oder den Remote-Zugang nicht nutzen wollen, klicken Sie auf **kein DynDNS**.
- 13) Klicken Sie auf **OK & Weiter**.

9.7.5.6 Wie Sie den Internet-Zugang deaktivieren

Voraussetzungen

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

Schritt für Schritt

- 1) Lassen Sie das Kontrollkästchen **Kein Internet-Zugang** aktiviert.
- 2) Klicken Sie auf **OK & Weiter**.

9.7.6 Internet-Telefonie

Im Fenster **Provider-Konfiguration und -Aktivierung für Internet-Telefonie** konfigurieren Sie die Internet-Telefonie. Sie können vorkonfigurierte oder neue Internet-Telefonie-Service-Provider (ITSP) konfigurieren. Für jeden ITSP können Sie einen oder mehrere Accounts konfigurieren. Es können bis zu 8 ITSP gleichzeitig aktiv sein.

Sie haben die folgenden 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 *Administratordokumentation, 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 Rufnummernband werden anschließend den internen Rufnummern der Teilnehmer manuell zugeordnet.

Die beiden Anschlussarten können kombiniert werden.

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

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

Somit ergeben sich die ITSP-Rufnummern aus der eingerichteten Anlagenrufnummer (z.B. Länderkennzahl 49) und den eingetragenen Durchwahlnummern im Langformat. Das hat Vorteile bei der Wahlbewertung und dem Call-Management, auch in einem Netzverbund. So ist der ITSP-Anschluss z.B. durchwahlfähig zu einem anderen Knoten.

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

9.7.6.1 Vordefinierten ITSP konfigurieren

Voraussetzungen

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

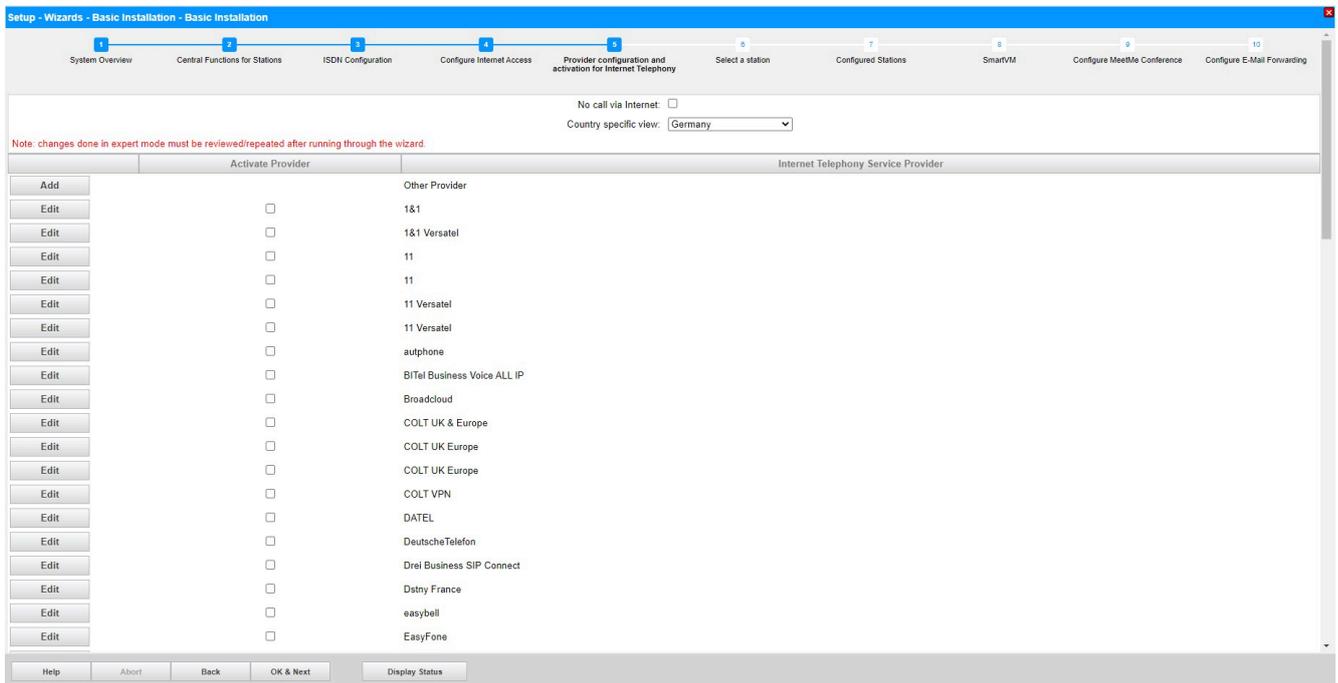
Die Verbindung zum Internet ist betriebsbereit.

Die Internet-Telefonie-Zugangsdaten Ihres ITSP liegen Ihnen vor (z. B. Benutzerkennung, Passwort, Internet-Telefonie-Rufnummern).

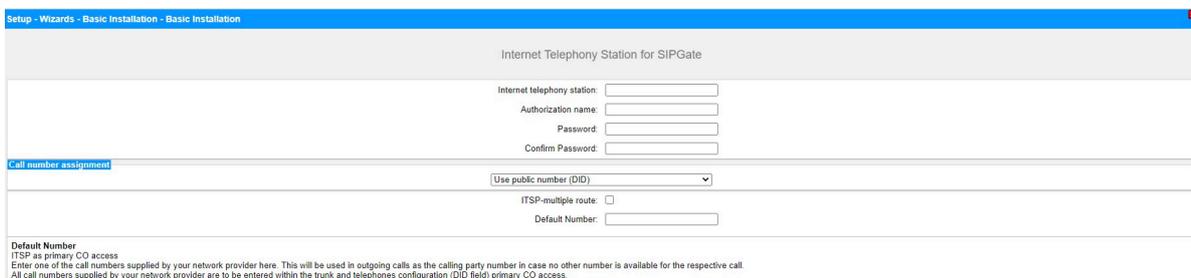
Schritt für Schritt

- 1) Deaktivieren Sie das Kontrollkästchen **Keine Telefonie über Internet**. Es wird Ihnen eine landesabhängige Liste der möglichen ITSP angezeigt.

Die Liste enthält die für das gewählte Land vordefinierten ITSP und die eventuell bereits angelegten ITSP.



- 2) Wenn Sie das voreingestellte Land ändern möchten, wählen Sie aus der Aufklappliste **Länderspezifische Ansicht** das gewünschte Land aus. Es werden die für das gewählte Land möglichen ITSP angezeigt.
- 3) Klicken Sie bei Bedarf auf **Status anzeigen**, um abzufragen, welche ITSP bereits aktiviert sind und welche Internet-Telefonie-Teilnehmer unter dem jeweiligen ITSP bereits eingerichtet sind. Maximal können Sie 8 ITSP aktivieren. Klicken Sie anschließend auf **OK**.
- 4) Klicken Sie in der Zeile des entsprechenden ITSP auf **Bearbeiten**, um einen vordefinierten ITSP zu konfigurieren.
- 5) Aktivieren Sie das Kontrollkästchen **Provider aktivieren**.
- 6) Klicken Sie auf **OK & Weiter**.
- 7) Klicken Sie auf **Hinzufügen**, um Ihre ITSP-Accounts mit den dazugehörigen Internet-Telefonie-Rufnummern zu konfigurieren. Die Felder, die Ihnen anschließend angezeigt werden, sind providerabhängig.

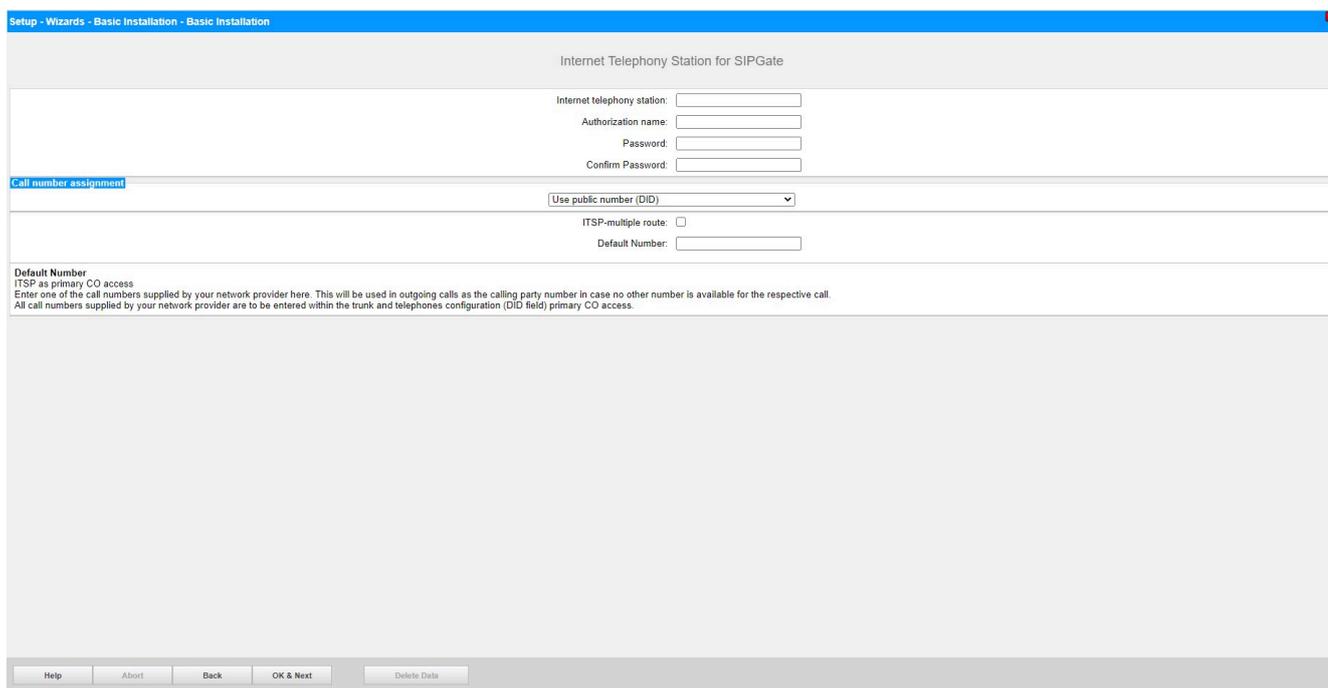


- 8) Geben im Feld **Internet-Telefonie-Teilnehmer** die Zugangsdaten Ihres Accounts ein. Die Daten haben Sie von Ihrem ITSP erhalten. Je nach ITSP werden hierfür unterschiedliche Bezeichnungen verwendet, wie z.B.: SIP-Benutzer, SIP-ID usw.
- 9) Geben Sie im Feld **Autorisierungsname** den Autorisierungsnamen ein. Die Daten haben Sie von Ihrem ITSP erhalten. Haben Sie keinen

Autorisierungsnamen erhalten, geben Sie die gleichen Daten wie unter **Internet-Telefonie-Teilnehmer** ein.

- 10) Geben Sie in den Feldern **Neues Kennwort** und **Kennwort wiederholen** das Kennwort an, das Sie vom ITSP erhalten haben. Je nach ITSP werden hierfür unterschiedliche Bezeichnungen verwendet, wie z.B.: Kennwort, SIP-Kennwort usw.
- 11) Zuordnung der Internet-Telefonie-Rufnummern - Möglichkeit 1:

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



- a) Wählen Sie im Bereich **Rufnummer-Zuordnung** das Optionsfeld **Öffentliche Rufnummer (DuWa)** aus.
- b) Geben Sie unter **Standard-Rufnummer** die Rufnummer ein, die bei gehenden Anrufen für Teilnehmer verwendet werden soll, die keine eigene Rufnummer haben.
- c) Falls Ihr ITSP das Leistungsmerkmal "Mobile Extension (MEX)" unterstützt, tragen Sie unter **MEX-Nummer** die vom ITSP zur Verfügung gestellte MEX-Nummer ein (8-stellig, nur Ziffern).
- 12) Zuordnung der Internet-Telefonie-Rufnummern - Möglichkeit 2:

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

- a) Wählen Sie im Bereich **Rufnummer-Zuordnung** das Optionsfeld **Interne Nummer (Rufnr.) verwenden / Einzeleinträge** aus.
- b) Geben Sie im Bereich **Internet-Telefonie-Teilnehmerrufnummern** im Feld neben der Schaltfläche **Hinzufügen** eine der vom ITSP mitgeteilten Internet-Telefonie-Teilnehmerrufnummern ein und klicken Sie auf **Hinzufügen**.

- c) Wenn Sie dem Account weitere Internet-Telefonie-Rufnummern zuordnen wollen, wiederholen Sie Schritt b).
- 13) Zuordnung der Internet-Telefonie-Rufnummern - Möglichkeit 3:**
- Interne Nummer (Rufnr.) verwenden / Bereichseintrag:** Sie besitzen einen Internet-Telefonie-Anlagenanschluss und haben als Internet-Telefonie-Rufnummern ein Rufnummernband erhalten, z.B. (+49) 89 7007-100 bis (+49) 89 7007-147. Sie weisen dann die Rufnummern aus dem Rufnummernbereich den internen Rufnummern der Teilnehmer zu.
- Wählen Sie im Bereich **Rufnummer-Zuordnung** das Optionsfeld **Interne Nummer (Rufnr.) verwenden / Bereichseintrag** aus.
 - Geben Sie unter **Anlagenrufnummer (Präfix)** die Anlagenrufnummer ein.
 - Geben Sie in den Feldern **Durchwahlband von** und **bis** das gewünschte Durchwahlband für den Internet-Telefonie-Teilnehmer ein. Standardmäßig ist 100 - 147 eingetragen.
- 14) Klicken Sie auf **OK & Weiter**.**
- 15) Wenn Sie weitere Accounts mit den dazugehörigen Internet-Telefonie-Rufnummern einrichten möchten, wiederholen Sie die Schritte 7 bis 14.**
- 16) Klicken Sie auf **OK & Weiter**.** Sie sehen eine Übersicht, welche Internet-Telefonie-Rufnummern welchen Accounts zugeordnet sind.
- 17) Ordnen Sie allen Internet-Telefonie-Rufnummern jeweils einer internen Rufnummer eines Teilnehmers zu.**

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

Name of Internet Telephony Station	Internet Telephony Phone Number	Internal Call Number	Use as PABX number for outgoing calls
0186136	75555555	<input type="checkbox"/> - 659995 Remote-Admin 659994 Licensing	<input type="checkbox"/>

- Wählen Sie in der entsprechenden Zeile aus der Aufklappliste **interne Rufnummer** eine interne Rufnummer aus.
 - Sollen Teilnehmer ohne Internet-Telefonie-Rufnummer oder Mitglieder einer Rufgruppe externe Telefonate über das Internet führen dürfen, muss das Optionsfeld **Als gehende Anlagenrufnummer verwenden** aktiviert sein. Das Optionsfeld kann ausschließlich bei einer einzigen Internet-Telefonie-Rufnummer aktiviert sein.
- 18) Klicken Sie auf **OK & Weiter**.** Hier sehen Sie nochmals die Liste der vordefinierten und neu hinzugefügten ITSP. Aktivierte ITSP sind in der Spalte **Provider aktivieren** mit einem Häkchen markiert. Mit **Restart ITSP** können Sie sich bei Verbindungsproblemen bei bereits aktivierten ITSP neu registrieren
- 19) Klicken Sie auf **OK & Weiter**.**
- 20) Geben Sie im Feld **Upstream bis zu (Kbit/s)** den Wert der Upload-Geschwindigkeit Ihrer Internet-Verbindung ein. Nicht zu verwechseln mit der Download-Geschwindigkeit!**

Anmerkung: Im Feld **Anzahl simultaner Internet-Telefongespräche** wird Ihnen die Anzahl der gleichzeitig

Ersteinrichtung von OpenScope Business X

zu führenden Internet-Telefongespräche angezeigt. Wenn sich auf Grund der Netzauslastung die Gesprächsqualität verschlechtert, müssen Sie die Anzahl reduzieren.

- 21) Klicken Sie auf **OK & Weiter**.
- 22) Falls Sie bei der Einrichtung Ihres Internet-Zugangs die Dauerverbindung noch nicht aktiviert haben, können Sie das hier nachholen. Ohne Dauerverbindung können Sie keine Anrufe über das Internet empfangen. Ist die Dauerverbindung bereits eingerichtet, erscheinen die unter a) bis c) beschriebenen Felder nicht.
 - a) Aktivieren Sie unter **Dauerverbindung** das Optionsfeld **An**.
 - b) Legen Sie im Feld **Zwangstrennung um (Std:Min)** die Uhrzeit fest, zu der die Internet-Verbindung getrennt werden soll (z. B. 04:59).
 - c) Klicken Sie auf **OK & Weiter**.
- 23) Tragen Sie in der Spalte **Gewählte Ziffern** die gewünschten Sonderrufnummern ein.

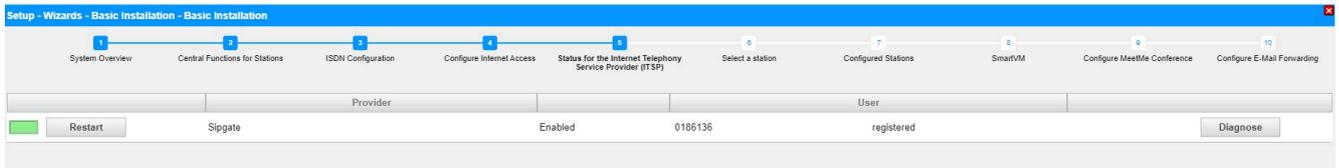
Special phone number	Dialed digits	Dial over Provider
1	@C112	Sipgate
2	@C110	Sipgate
3	@C0137Z	Sipgate
4	@C0136Z	Sipgate
5	@C0900Z	Sipgate
6	@C118Z	Sipgate
7	@C116Z	Sipgate
8	@C115	Sipgate
9	@C010Z	Sipgate

Folgende Rufnummerneinträge sind gültig:

- 0 bis 9: Zulässige Ziffern
 - -: Feldtrennzeichen
 - X: beliebige Ziffer von 0 bis 9
 - N: beliebige Ziffer von 2 bis 9
 - Z: Eine oder mehrere Ziffern folgen bis Wahlende
 - C: Simulierter Wählton (kann max. dreimal eingetragen werden)
- 24) Wählen Sie in der Spalte **Wählen über Provider** aus, ob die Sonderrufnummer über ISDN oder über einen ITSP gewählt werden soll. Es werden nur aktive ITSP angezeigt.

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

25) Klicken Sie auf **OK & Weiter**. Der Status Ihres ITSP wird angezeigt.



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

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

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

9.7.6.2 Wie Sie die Internet-Telefonie deaktivieren

Voraussetzungen

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

Schritt für Schritt

- 1) Lassen Sie das Kontrollkästchen **Keine Telefonie über Internet** aktiviert.
- 2) Klicken Sie zweimal auf **OK & Weiter**.

9.7.7 Teilnehmer

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

Gehen Sie folgendermaßen vor:

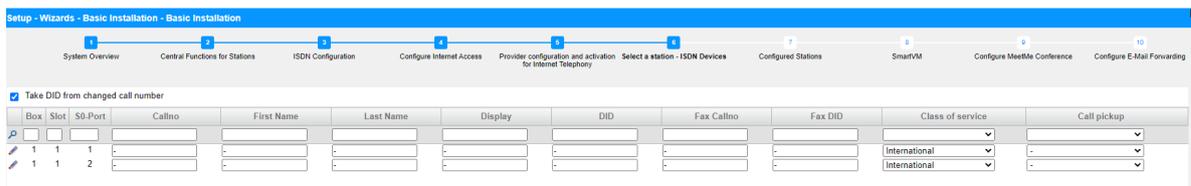
- 1) ISDN-Teilnehmer konfigurieren
ISDN-Teilnehmer sind z.B. ISDN-Telefone oder ISDN-Faxgeräte. ISDN-Teilnehmer können Sie nur konfigurieren, wenn Sie eine S₀-Schnittstelle als internen S₀-Anschluss konfiguriert haben.
- 2) Analoge Teilnehmer konfigurieren
Analoge Teilnehmer sind z.B. analoge Telefone 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 *Administratordokumentation, Konfiguration der integrierten Cordless-Lösung*
- 5) IP- und SIP-Teilnehmer konfigurieren
IP-Teilnehmer und SIP-Teilnehmer sind z.B. LAN-Telefone oder WLAN-Telefone.

9.7.7.1 ISDN-Teilnehmer konfigurieren

Voraussetzungen

Sie befinden sich im Fenster **Teilnehmer auswählen - ISDN-Endgeräte**.

Die S₀-Anschlüsse, an denen die ISDN-Telefone angeschlossen sind, müssen als interner S₀-Anschluss eingerichtet sein.



Schritt für Schritt

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

- Nur bei Anlagenanschluss:

Klicken Sie in das gewünschte Feld und geben Sie über die Tastatur die Durchwahlnummer ein. Die Durchwahlnummer kann auch mit der internen Rufnummer identisch sein.

- Nur bei Mehrgeräteanschluss:

Wählen Sie in dem gewünschten Feld über die Aufklappliste eine MSN aus. Der Teilnehmer kann z.B. von intern über die interne Rufnummer 101 und von extern über die MSN 654321 erreicht werden.

- Bei Anlagenanschluss und Mehrgeräteanschluss:

Wählen Sie in dem gewünschten Feld über die Aufklappliste den Eintrag **xxx - änderbar** aus (xxx steht für die interne Rufnummer) und geben Sie über die Tastatur die Durchwahlnummer ein oder wählen Sie über die Aufklappliste eine MSN aus.

2) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Rufnr** eine interne Rufnummer für den Teilnehmer ein. Sie können die vorbelegte Rufnummer verwenden oder eine andere, noch nicht belegte Rufnummer vergeben.

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

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

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

- Geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax Rufnr** die gewünschte interne Fax-Rufnummer ein, unter der der Teilnehmer von intern Faxnachrichten empfangen kann.
- Wenn für die Faxbox eine Durchwahlnummer konfiguriert werden soll, geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax**

Durchwahl die gewünschte externe Fax-Rufnummer ein, unter der der Teilnehmer von extern Faxnachrichten empfangen kann.

- 5) Wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Berechtigung** die gewünschte Berechtigungsgruppe aus.
- 6) Um den Teilnehmer in eine Anrufübernahmegruppe aufzunehmen, wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Anrufübernahme** eine Anrufübernahmegruppe aus.
- 7) Führen Sie die unter diesem Schritt beschriebenen Einstellungen nur bei Bedarf durch:
 - a) Klicken Sie in der Zeile des gewünschten ISDN-Teilnehmers auf das Stiftsymbol **Bearbeiten**.

- b) Geben Sie im Feld **Clip/Lin** eine Rufnummer ein (Durchwahlnummer oder MSN), die beim einem externen Anruf im Display des Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird.

Anmerkung: Dieses Leistungsmerkmal muss vom Netzanbieter freigegeben sein.

Anmerkung: Es sollte mindestens eine DuWa-Nummer konfiguriert werden. Wenn dies nicht der Fall ist, berücksichtigt das System die CLIP-Nummer des Anrufers nicht und die interne Rufnummer wird formatiert und als die Nummer des anrufenden Teilnehmers für den externen Anruf gesendet.

- c) Wählen Sie aus der Aufklappliste **Stationstyp** den Typ des ISDN-Endgeräts aus.
- d) Wählen Sie im Bereich **Durchwahl für Internet-Telefonie** aus einer Aufklappliste eine Durchwahlnummer aus. Für jeden aktiven ITSP wird Ihnen eine Aufklappliste angezeigt.

Anmerkung: Das Feld **Durchwahl für Internet-Telefonie** ist nicht sichtbar, wenn die Internet-Telefonie

nicht eingerichtet oder kein Internet-Telefonie-Service-Provider aktiviert ist.

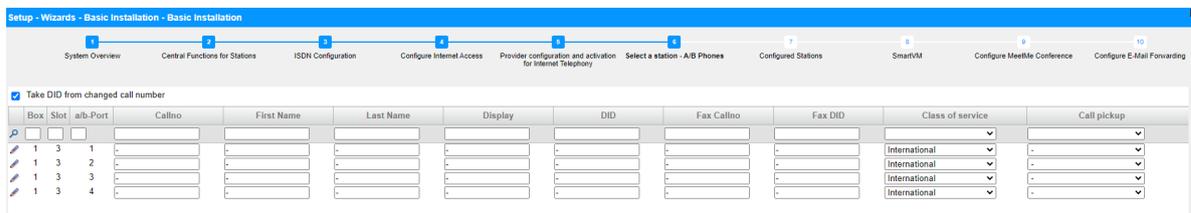
- e) Weisen Sie aus der Aufklappliste **Rufsignalisierung intern** dem Teilnehmer eine von insgesamt acht möglichen akustischen Rufsignalisierungen für interne Anrufe zu. Dadurch sendet der Teilnehmer anderen internen Teilnehmern einen veränderten Rufton, durch den er von anderen Teilnehmern unterschieden werden kann (Standard: Rufart 1).
- f) Weisen Sie aus der Aufklappliste **Rufsignalisierung extern** dem Teilnehmer eine von insgesamt drei möglichen akustischen Rufsignalisierungen für externe Anrufe zu (Standard: Rufart 1).
- g) Klicken Sie auf **OK & Weiter**.
- h) Ändern Sie bei Bedarf die Teilnehmer-Flags. Für eine Beschreibung der Teilnehmer-Flags siehe *Administratordokumentation, Teilnehmer > Teilnehmer > Teilnehmer-Parameter*.
- i) Klicken Sie auf **OK & Weiter**.
- 8) Wenn Sie weitere ISDN-Teilnehmer einrichten möchten, klicken Sie auf **Daten speichern** und wiederholen Sie die Schritte 1 bis 7.
- 9) Klicken Sie auf **OK & Weiter**.

9.7.7.2 Analoge Teilnehmer konfigurieren

Voraussetzungen

Sie befinden sich im Fenster **Teilnehmer auswählen - A/B-Endgeräte**.

Ein Mainboard oder eine Baugruppe mit analogen Schnittstellen ist vorhanden.



Schritt für Schritt

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

Klicken Sie in das gewünschte Feld und geben Sie über die Tastatur die Durchwahlnummer ein. Die Durchwahlnummer kann auch mit der internen Rufnummer identisch sein.
 - Nur bei Mehrgeräteanschluss:

Wählen Sie in dem gewünschten Feld über die Aufklappliste eine MSN aus. Der Teilnehmer kann z.B. von intern über die interne Rufnummer 101 und von extern über die MSN 654321 erreicht werden.
 - Bei Anlagenanschluss und Mehrgeräteanschluss:

Wählen Sie in dem gewünschten Feld über die Aufklappliste den Eintrag **xxx - änderbar** aus (xxx steht für die interne Rufnummer) und geben Sie über die Tastatur die Durchwahlnummer ein oder wählen Sie über die Aufklappliste eine MSN aus.
- 2) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Rufnr** eine interne Rufnummer für den Teilnehmer ein. Sie können die vorbelegte Rufnummer verwenden oder eine andere, noch nicht belegte Rufnummer vergeben.
- 3) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Name** einen Namen in der Form *Nachname, Vorname* oder *Vorname Nachname* ein.

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

- 4) Wenn für den Teilnehmer eine Faxbox eingerichtet werden soll (nutzbar z.B. mit den UC Clients **myPortal for Desktop** oder **myPortal for Outlook**), gehen Sie folgendermaßen vor:
 - a) Geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax Rufnr** die gewünschte interne Fax-Rufnummer ein, unter der der Teilnehmer von intern Faxnachrichten empfangen kann.
 - b) Wenn für die Faxbox eine Durchwahlnummer konfiguriert werden soll, geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax DuWa** die gewünschte externe Fax-Rufnummer ein, unter der der Teilnehmer von extern Faxnachrichten empfangen kann.
- 5) Wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Berechtigung** die gewünschte Berechtigungsgruppe aus.
- 6) Um den Teilnehmer in eine Anrufübernahmegruppe aufzunehmen, wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Anrufübernahme** eine Anrufübernahmegruppe aus.

- 7) Führen Sie die unter diesem Schritt beschriebenen Einstellungen nur bei Bedarf durch:
- a) Klicken Sie in der Zeile des gewünschten analogen Teilnehmers auf das Stiftsymbol **Bearbeiten**.

- b) Geben Sie im Feld **Clip/Lin** eine Rufnummer ein (Durchwahlnummer oder MSN), die beim einem externen Anruf im Display des Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird.

Anmerkung: Dieses Leistungsmerkmal muss vom Netzanbieter freigegeben sein.

Anmerkung: Es sollte mindestens eine DuWa-Nummer konfiguriert werden. Wenn dies nicht der Fall ist, berücksichtigt das System die CLIP-Nummer des Anrufers nicht und die interne Rufnummer wird formatiert und als die Nummer des anrufenden Teilnehmers für den externen Anruf gesendet.

- c) Wählen Sie aus der Aufklappliste **Stationstyp** den Typ des analogen Endgeräts (z. B. Fax) aus.
- d) Wählen Sie im Bereich **Durchwahl für Internet-Telefonie** aus einer Aufklappliste eine Durchwahlnummer aus. Für jeden aktiven ITSP wird Ihnen eine Aufklappliste angezeigt.

Anmerkung: Das Feld **Durchwahl für Internet-Telefonie** ist nicht sichtbar, wenn die Internet-Telefonie nicht eingerichtet oder kein Internet-Telefonie-Service-Provider aktiviert ist.

- e) Weisen Sie aus der Aufklappliste **Rufsignalisierung intern** dem Teilnehmer eine von insgesamt acht möglichen akustischen Rufsignalisierungen für interne Anrufe zu. Dadurch sendet der Teilnehmer anderen internen Teilnehmern einen veränderten Rufton, durch den

er von anderen Teilnehmern unterschieden werden kann (Standard: Rufart 1).

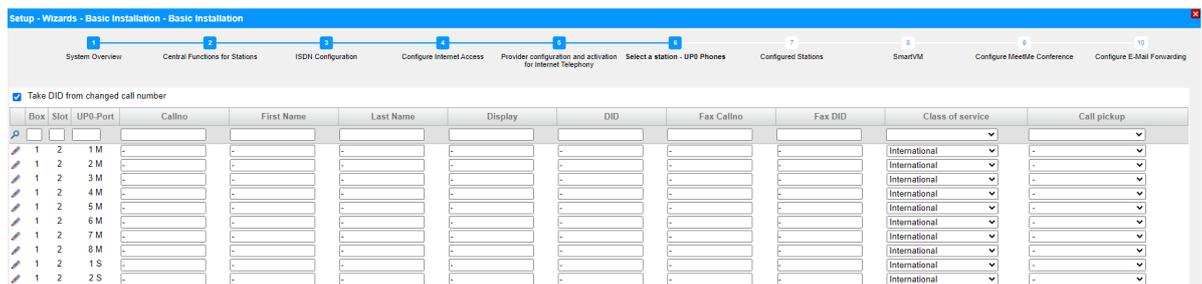
- f) Weisen Sie aus der Aufklappliste **Rufsignalisierung extern** dem Teilnehmer eine von insgesamt drei möglichen akustischen Rufsignalisierungen für externe Anrufe zu (Standard: Rufart 1).
 - g) Klicken Sie auf **OK & Weiter**.
 - h) Ändern Sie bei Bedarf die Teilnehmer-Flags. Für eine Beschreibung der Teilnehmer-Flags siehe *Administratordokumentation, Teilnehmer > Teilnehmer > Teilnehmer-Parameter*.
 - i) Klicken Sie auf **OK & Weiter**.
- 8) Wenn Sie einen weiteren analogen Teilnehmer einrichten möchten, klicken Sie auf **Daten speichern** und wiederholen Sie die Schritte 1 bis 7.
- 9) Klicken Sie auf **OK & Weiter**.

9.7.7.3 UP0-Teilnehmer konfigurieren

Voraussetzungen

Sie befinden sich im Fenster **Teilnehmer auswählen - UP0-Endgeräte**.

Ein Mainboard oder eine Baugruppe mit UP0-Schnittstellen ist vorhanden.



Schritt für Schritt

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

Klicken Sie in das gewünschte Feld und geben Sie über die Tastatur die Durchwahlnummer ein. Die Durchwahlnummer kann auch mit der internen Rufnummer identisch sein.
 - Nur bei Mehrgeräteanschluss:

Wählen Sie in dem gewünschten Feld über die Aufklappliste eine MSN aus. Der Teilnehmer kann z.B. von intern über die interne Rufnummer 101 und von extern über die MSN 654321 erreicht werden.
 - Bei Anlagenanschluss und Mehrgeräteanschluss:

Wählen Sie in dem gewünschten Feld über die Aufklappliste den Eintrag **xxx - änderbar** aus (xxx steht für die interne Rufnummer) und geben Sie über die Tastatur die Durchwahlnummer ein oder wählen Sie über die Aufklappliste eine MSN aus.
- 2) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Rufnr** eine interne Rufnummer für den Teilnehmer ein. Sie können die vorbelegte

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

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

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

- 4) Wenn für den Teilnehmer eine Faxbox eingerichtet werden soll (nutzbar z.B. mit den UC Clients **myPortal for Desktop** oder **myPortal for Outlook**), gehen Sie folgendermaßen vor:
- a) Geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax Rufnr** die gewünschte interne Fax-Rufnummer ein, unter der der Teilnehmer von intern Faxnachrichten empfangen kann.
 - b) Wenn für die Faxbox eine Durchwahlnummer konfiguriert werden soll, geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax Durchwahl** die gewünschte externe Fax-Rufnummer ein, unter der der Teilnehmer von extern Faxnachrichten empfangen kann.
- 5) Wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Berechtigung** die gewünschte Berechtigungsgruppe aus.
- 6) Um den Teilnehmer in eine Anrufübernahmegruppe aufzunehmen, wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Anrufübernahme** eine Anrufübernahmegruppe aus.

- 7) Führen Sie die unter diesem Schritt beschriebenen Einstellungen nur bei Bedarf durch:
- a) Klicken Sie in der Zeile des gewünschten Teilnehmers auf das Stiftsymbol **Bearbeiten**.

- b) Geben Sie im Feld **Clip/Lin** eine Rufnummer ein (Durchwahlnummer oder MSN), die beim einem externen Anruf im Display des Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird.

Anmerkung: Dieses Leistungsmerkmal muss vom Netzanbieter freigegeben sein.

Anmerkung: Es sollte mindestens eine DuWa-Nummer konfiguriert werden. Wenn dies nicht der Fall ist, berücksichtigt das System die CLIP-Nummer des Anrufers nicht und die interne Rufnummer wird formatiert und als die Nummer des anrufenden Teilnehmers für den externen Anruf gesendet.

- c) Wählen Sie aus der Aufklappliste **Stationstyp** den Typ des TDM-Endgeräts aus.
- d) Belassen Sie die Standard-Auswahl in der Aufklappliste **Sprache**. Für TDM-Endgeräte ist diese Einstellung ohne Bedeutung.
- e) Wählen Sie im Bereich **Durchwahl für Internet-Telefonie** aus einer Aufklappliste eine Durchwahlnummer aus. Für jeden aktiven ITSP wird Ihnen eine Aufklappliste angezeigt.

Anmerkung: Das Feld **Durchwahl für Internet-Telefonie** ist nicht sichtbar, wenn die Internet-Telefonie nicht eingerichtet oder kein Internet-Telefonie-Service-Provider aktiviert ist.

- f) Weisen Sie aus der Aufklappliste **Rufsignalisierung intern** dem Teilnehmer eine von insgesamt acht möglichen akustischen Rufsignalisierungen für interne Anrufe zu. Dadurch sendet der Teilnehmer anderen internen Teilnehmern einen veränderten Ruftönen, durch den

Ersteinrichtung von OpenScape Business X

er von anderen Teilnehmern unterschieden werden kann (Standard: Rufart 1).

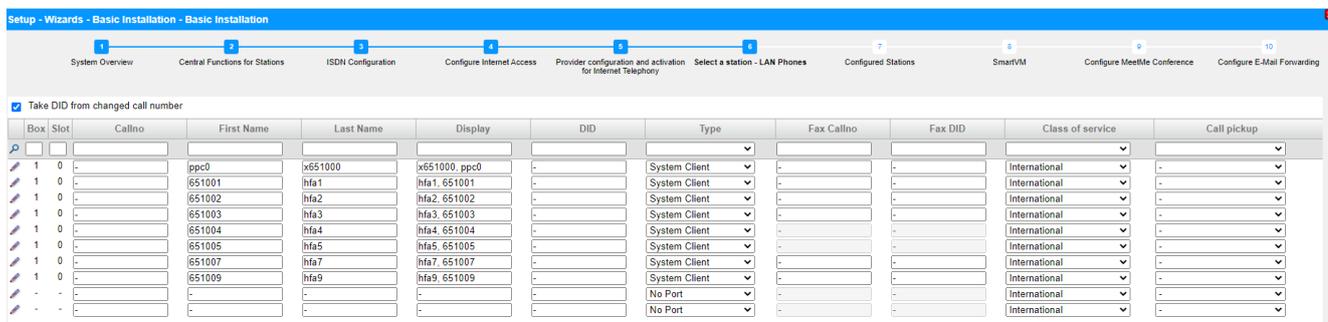
- g) Weisen Sie aus der Aufklappliste **Rufsignalisierung extern** dem Teilnehmer eine von insgesamt drei möglichen akustischen Rufsignalisierungen für externe Anrufe zu (Standard: Rufart 1).
 - h) Klicken Sie auf **OK & Weiter**.
 - i) Ändern Sie bei Bedarf die Teilnehmer-Flags. Für eine Beschreibung der Teilnehmer-Flags siehe *Administratordokumentation, Teilnehmer > Teilnehmer > Teilnehmer-Parameter*.
 - j) Klicken Sie auf **OK & Weiter**.
- 8) Wenn Sie einen weiteren UP0-Teilnehmer einrichten möchten, klicken Sie auf **Daten speichern** und wiederholen Sie die Schritte 1 bis 7.
- 9) Klicken Sie auf **OK & Weiter**.

9.7.7.4 Wie Sie DECT-Teilnehmer konfigurieren

Voraussetzungen

Sie befinden sich im Fenster **Teilnehmer auswählen - DECT-Endgeräte** im Assistenten für die **Grundinstallation**.

Für die Konfiguration von DECT-Teilnehmern muss eine Basisstation angeschlossen und die DECT-Telefone dort angemeldet sein. Ist dies nicht der Fall, überspringen Sie dieses Fenster. Sie können die DECT-Teilnehmer auch später noch konfigurieren (siehe *Administratordokumentation, Konfiguration der Teilnehmer*).



Schritt für Schritt

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

Klicken Sie in das gewünschte Feld und geben Sie über die Tastatur die Durchwahlnummer ein. Die Durchwahlnummer kann auch mit der internen Rufnummer identisch sein.
 - Nur bei Mehrgeräteanschluss:

Wählen Sie in dem gewünschten Feld über die Aufklappliste eine MSN aus. Der Teilnehmer kann z.B. von intern über die interne Rufnummer 101 und von extern über die MSN 654321 erreicht werden.
 - Bei Anlagenanschluss und Mehrgeräteanschluss:

Wählen Sie in dem gewünschten Feld über die Aufklappliste den Eintrag **xxx - änderbar** aus (xxx steht für die interne Rufnummer) und geben Sie über die Tastatur die Durchwahlnummer ein oder wählen Sie über die Aufklappliste eine MSN aus.
- 2) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Rufnr** eine interne Rufnummer für den Teilnehmer ein. Sie können die vorgelegte Rufnummer verwenden oder eine andere, noch nicht belegte Rufnummer vergeben.
- 3) Wenn für den Teilnehmer eine Faxbox eingerichtet werden soll (nutzbar z.B. mit den UC Clients **myPortal for Desktop** oder **myPortal for Outlook**), gehen Sie folgendermaßen vor:
 - a) Geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax Rufnr** die gewünschte interne Fax-Rufnummer ein, unter der der Teilnehmer von intern Faxnachrichten empfangen kann.
 - b) Wenn für die Faxbox eine Durchwahlnummer konfiguriert werden soll, geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax Durchwahl** die gewünschte externe Fax-Rufnummer ein, unter der der Teilnehmer von extern Faxnachrichten empfangen kann.
- 4) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Name** einen Namen in der Form `Nachname, Vorname` oder `Vorname Nachname` ein.

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

- 5) Wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Berechtigung** die gewünschte Berechtigungsgruppe aus.
- 6) Um den Teilnehmer in eine Anrufübernahmegruppe aufzunehmen, wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Anrufübernahme** eine Anrufübernahmegruppe aus.
- 7) Falls Sie den DECT-Telefoncode (PIN) ändern wollen, geben Sie in der Zeile des gewünschten Teilnehmers unter **Mobilcode** den neuen Code ein. Der DECT-Teilnehmer muss sich mit diesem Code neu an der Basisstation anmelden.

Ersteinrichtung von OpenScape Business X

8) Führen Sie die unter diesem Schritt beschriebenen Einstellungen nur bei Bedarf durch:

a) Klicken Sie in der Zeile des gewünschten Teilnehmers auf das Stiftsymbol **Bearbeiten**.

b) Geben Sie im Feld **Clip/Lin** eine Rufnummer ein (Durchwahlnummer oder MSN), die beim einem externen Anruf im Display des Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird.

Anmerkung: Dieses Leistungsmerkmal muss vom Netzanbieter freigegeben sein.

Anmerkung: Es sollte mindestens eine DuWa-Nummer konfiguriert werden. Wenn dies nicht der Fall ist, berücksichtigt das System die CLIP-Nummer des Anrufers nicht und die interne Rufnummer wird formatiert und als die Nummer des anrufenden Teilnehmers für den externen Anruf gesendet.

- c) Wählen Sie aus der Aufklappliste **Stationstyp** den Typ des Schnurlos-Endgeräts aus.
- d) Belassen Sie die Standard-Auswahl in der Aufklappliste **Sprache**. Für Schnurlos-Endgeräte ist diese Einstellung ohne Bedeutung.
- e) Wählen Sie im Bereich **Durchwahl für Internet-Telefonie** aus einer Aufklappliste eine Durchwahlnummer aus. Für jeden aktiven ITSP wird Ihnen eine Aufklappliste angezeigt.

Anmerkung: Das Feld **Durchwahl für Internet-Telefonie** ist nicht sichtbar, wenn die Internet-Telefonie

nicht eingerichtet oder kein Internet-Telefonie-Service-Provider aktiviert ist.

- f) Weisen Sie aus der Aufklappliste **Rufsignalisierung intern** dem Teilnehmer eine von insgesamt acht möglichen akustischen Rufsignalisierungen für interne Anrufe zu. Dadurch sendet der Teilnehmer anderen internen Teilnehmern einen veränderten Ruftton, durch den er von anderen Teilnehmern unterschieden werden kann (Standard: Rufart 1).
 - g) Weisen Sie aus der Aufklappliste **Rufsignalisierung extern** dem Teilnehmer eine von insgesamt drei möglichen akustischen Rufsignalisierungen für externe Anrufe zu (Standard: Rufart 1).
 - h) Klicken Sie auf **OK & Weiter**.
 - i) Ändern Sie bei Bedarf die Teilnehmer-Flags. Für eine Beschreibung der Teilnehmer-Flags siehe *Administratordokumentation, Teilnehmer > Teilnehmer > Teilnehmer-Parameter*.
 - j) Klicken Sie auf **OK & Weiter**.
- 9) Wenn Sie einen weiteren Teilnehmer einrichten möchten, klicken Sie auf **Daten speichern** und wiederholen Sie die Schritte 1 bis 8.
- 10) Klicken Sie auf **OK & Weiter**.

9.7.7.5 Wie Sie IP- und SIP-Teilnehmer konfigurieren

Voraussetzungen

Sie befinden sich im Fenster **Teilnehmer auswählen - LAN-Telefone**.

Für den Betrieb von WLAN-Telefonen benötigen Sie ein funktionsfähiges Wireless LAN-Netzwerk.

Setup - Wizards - Telephones / Subscribers - IP Telephones

Select a station -LAN Phones/WLAN Phones

Take DID from changed call number

Box	Slot	Callno	First Name	Last Name	Display	DID	Type	Fax Callno	Fax DID	Class of service	Call pickup
1	0		ppc0	x651000	x651000_ppc0	-	System Client			International	-
1	0	651001	hfa1	hfa1	hfa1_651001	-	System Client			International	-
1	0	651002	hfa2	hfa2	hfa2_651002	-	System Client			International	-
1	0	651003	hfa3	hfa3	hfa3_651003	-	System Client			International	-
1	0	651004	hfa4	hfa4	hfa4_651004	-	System Client			International	-
1	0	651005	hfa5	hfa5	hfa5_651005	-	System Client			International	-
1	0	651007	hfa7	hfa7	hfa7_651007	-	System Client			International	-
1	0	651009	hfa9	hfa9	hfa9_651009	-	System Client			International	-
-	-						No Port			International	-
-	-						No Port			International	-

Schritt für Schritt

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

Klicken Sie in das gewünschte Feld und geben Sie über die Tastatur die Durchwahlnummer ein. Die Durchwahlnummer kann auch mit der internen Rufnummer identisch sein.
 - Nur bei Mehrgeräteanschluss:

Wählen Sie in dem gewünschten Feld über die Aufklappliste eine MSN aus. Der Teilnehmer kann z.B. von intern über die interne Rufnummer 101 und von extern über die MSN 654321 erreicht werden.
 - Bei Anlagenanschluss und Mehrgeräteanschluss:

Wählen Sie in dem gewünschten Feld über die Aufklappliste den Eintrag **xxx - änderbar** aus (xxx steht für die interne Rufnummer) und geben Sie über die Tastatur die Durchwahlnummer ein oder wählen Sie über die Aufklappliste eine MSN aus.
- 2) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Rufnr** eine interne Rufnummer für den Teilnehmer ein. Sie können die vorbelegte Rufnummer verwenden oder eine andere, noch nicht belegte Rufnummer vergeben.
- 3) Geben Sie in der Zeile des gewünschten Teilnehmers unter **Name** einen Namen in der Form *Nachname, Vorname* ein.

Anmerkung: Der Name kann aus bis zu 16 Zeichen bestehen, sollte aber keine Umlaute oder Sonderzeichen enthalten. Der Name wird wie hier angegeben bei den UC Clients als Nachname eingetragen, kann dort aber nachbearbeitet werden.

- 4) Wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Typ** den Typ des IP-Teilnehmers aus (z. B. "System Client" oder "SIP Client").
- 5) Wenn für den Teilnehmer eine Faxbox eingerichtet werden soll (nutzbar z.B. mit den UC Clients **myPortal for Desktop** oder **myPortal for Outlook**), gehen Sie folgendermaßen vor:
 - a) Geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax Rufnr** die gewünschte interne Fax-Rufnummer ein, unter der der Teilnehmer von intern Faxnachrichten empfangen kann.
 - b) Wenn für die Faxbox eine Durchwahlnummer konfiguriert werden soll, geben Sie in der Zeile des gewünschten Teilnehmers im Feld **Fax Durchwahl** die gewünschte externe Fax-Rufnummer ein, unter der der Teilnehmer von extern Faxnachrichten empfangen kann.
- 6) Wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Berechtigung** die gewünschte Berechtigungsgruppe aus.
- 7) Um den Teilnehmer in eine Anrufübernahmegruppe aufzunehmen, wählen Sie in der Zeile des gewünschten Teilnehmers aus der Aufklappliste **Anrufübernahme** eine Anrufübernahmegruppe aus.

- 8) Führen Sie die unter diesem Schritt beschriebenen Einstellungen nur bei Bedarf oder für ein SIP-Telefon durch:
- a) Klicken Sie in der Zeile des gewünschten Teilnehmers auf das Stiftsymbol **Bearbeiten**.

- b) Für SIP-Telefone: Wenn das SIP-Telefon zusammen mit einem Dual-Mode-Mobiltelefon betrieben werden soll, geben Sie im Bereich **Mobility** unter **mobile Rufnummer** die Amtskennziffer und gefolgt von der Rufnummer des Mobiltelefons ein (z.B. 0016012345678). Wählen Sie zusätzlich aus der Aufklappliste **Web Feature ID** diesen SIP Client aus. (siehe *Administratordokumentation, Dual-Mode-Telefonie*).
- c) Geben Sie im Feld **Clip/Lin** eine Rufnummer ein (Durchwahlnummer oder MSN), die beim einem externen Anruf im Display des Angerufenen an Stelle der eigentlichen Rufnummer angezeigt wird.

Anmerkung: Dieses Leistungsmerkmal muss vom Netzanbieter freigegeben sein.

Anmerkung: Es sollte mindestens eine DuWa-Nummer konfiguriert werden. Wenn dies nicht der Fall ist, berücksichtigt das System die CLIP-Nummer des Anrufers nicht und die interne Rufnummer wird formatiert und als die Nummer des anrufenden Teilnehmers für den externen Anruf gesendet.

- d) Wählen Sie aus der Aufklappliste **Sprache** die Sprache für die Menüsteuerung des Telefons aus.
- e) Weisen Sie aus der Aufklappliste **Rufsignalisierung intern** dem Teilnehmer eine von insgesamt acht möglichen akustischen Rufsignalisierungen für interne Anrufe zu. Dadurch sendet der Teilnehmer anderen internen Teilnehmern einen veränderten Rufton, durch den er von anderen Teilnehmern unterschieden werden kann (Standard: Rufart 1).

- f) Weisen Sie aus der Aufklappliste **Rufsignalisierung extern** dem Teilnehmer eine von insgesamt drei möglichen akustischen Rufsignalisierungen für externe Anrufe zu (Standard: Rufart 1).
 - g) Nur für SIP-Telefone: Aktivieren Sie das Kontrollkästchen **Authentifizierung aktiv**.
 - h) Nur für SIP-Telefone: Geben Sie im Feld **Passwort** und im Feld **Passwort bestätigen** das Authentifizierungspasswort ein.
 - i) Nur für SIP-Telefone: Geben Sie im Feld **SIP User ID / Benutzername** die Benutzererkennung für die Authentifizierung ein.
 - j) Nur für SIP-Telefone: Geben Sie im Feld **Realm** die zugehörige Zone für die Authentifizierung ein.
 - k) Klicken Sie auf **OK & Weiter**.
 - l) Ändern Sie bei Bedarf die Teilnehmer-Flags. Für eine Beschreibung der Teilnehmer-Flags siehe *Administratorokumentation, Teilnehmer > Teilnehmer > Teilnehmer-Parameter*.
 - m) Klicken Sie auf **OK & Weiter**.
- 9) Wenn Sie einen weiteren IP-Teilnehmer einrichten möchten, klicken Sie auf **Daten speichern** und wiederholen Sie die Schritte 1 bis 8.
- 10) Klicken Sie auf **OK & Weiter**. Sie sehen eine Liste aller eingerichteten Teilnehmer. Diese Liste entspricht einem Rufnummernplan.
- 11) Klicken Sie bei Bedarf auf **Drucken**, um die Daten der eingerichteten Teilnehmer auszudrucken.
- 12) Klicken Sie anschließend auf **OK & Weiter**.

9.7.8 Konfiguration von UC Suite

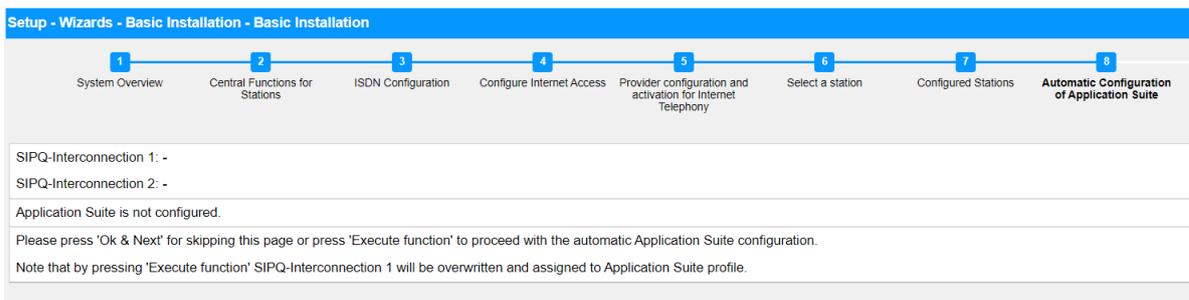
Im Fenster **Automatische Konfiguration der Applikation-Suite** können Sie die automatische Konfiguration der UC-Lösung UC Suite durchführen.

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

9.7.8.1 Wie Sie UC Suite konfigurieren

Voraussetzungen

Sie befinden sich im Fenster **Automatische Konfiguration der Application Suite**.



Schritt für Schritt

- 1) Wenn keine UC Booster Card in das Kommunikationssystem integriert ist, klicken Sie auf **OK & Weiter**. Die Konfiguration wird übersprungen.
- 2) Wenn die UC Booster Card in das Kommunikationssystem integriert ist, klicken Sie auf **Funktion ausführen**. Die UC Suite wird automatisch konfiguriert. Sobald der Verlaufs balken 100% anzeigt, klicken Sie auf **OK & Weiter**.

9.7.9 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.

9.7.9.1 Wie Sie die UC Smart Sprachboxen konfigurieren**Voraussetzungen**

Sie befinden sich im Fenster **Automatische Konfiguration von Smart VM**.

Setup - Wizards - Basic Installation - Basic Installation

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

- The automatic Smart VM configuration is an initial configuration and generates the necessary data to setup voicemail boxes or can be used to recover existing mailboxes with default settings. If there are already existing voicemail or autoattendant mailboxes, then all mailbox data will be deleted irrevocably! This affects also mailboxes created by the xmi-import. If the corresponding intercept position call number (Smart VM) is configured, a mailbox is created for that intercept position. If the corresponding autoattendant call number (Smart VM) is configured, a mailbox is created for that autoattendant. A mailbox is created for each of the first 99 stations. MeetMe station needs to be already configured in order for a MeetMe mailbox to be created. The second group/hunt group, used for Smart VM, is recovered with default data. The third group/hunt group, used for autoattendant, is recovered with default data.
- Press "Execute function" to proceed with Smart VM configuration or press "OK & Next" for skipping this page.

Schritt für Schritt

- 1) Wenn die UC Smart Sprachboxen nicht genutzt werden sollen, klicken Sie auf **OK & Weiter**. Die Konfiguration der Sprachboxen wird übersprungen.
- 2) Wenn die UC Smart Sprachboxen genutzt werden sollen, klicken Sie auf **Funktion ausführen**. Für die ersten 100 Teilnehmer werden automatisch Sprachboxen konfiguriert. Sobald der Verlaufs balken 100% anzeigt, klicken Sie auf **OK & Weiter**.

Anmerkung: Bereits vorhandene UC Smart Sprachboxen oder UC Smart AutoAttendant-Sprachboxen werden dabei unwiderruflich gelöscht.

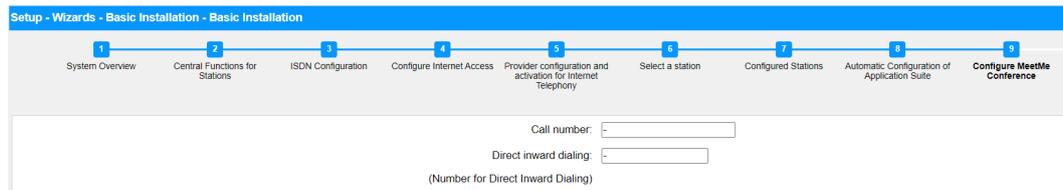
9.7.10 Konferenz-Server-Einstellungen

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

9.7.10.1 Wie Sie die Konferenz-Server-Einstellungen ändern

Voraussetzungen

Sie befinden sich im Fenster **MeetMe-Konferenz-Einstellungen ändern**.



Schritt für Schritt

- 1) Geben Sie im Feld **Rufnummer** eine Rufnummer für die Konferenz ein.
- 2) Legen Sie im Feld **Durchwahl** die Einwahlnummer für die Konferenz (Konferenz-DUWA) fest, mit der sich Teilnehmer in eine bestehende Konferenz einwählen können.
- 3) Klicken Sie auf **OK & Weiter**.

9.7.11 E-Mail-Versand (optional)

Im Fenster **E-Mail-Weiterleitung ändern** können Sie den E-Mail-Versand konfigurieren. Teilnehmer werden dadurch über neue Sprach- und Faxnachrichten informiert und der Administrator erhält Systemmeldungen.

Sie haben die folgenden 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.

9.7.11.1 E-Mail-Versand konfigurieren

Voraussetzungen

Wenn der externe E-Mail-Server für die Verwendung der einfachen Authentifizierung konfiguriert wurde, stellen Sie sicher, dass ein E-Mail-

Konto mit Kennwort bei einem E-Mail-Anbieter vorhanden ist und Sie die Zugangsdaten für dieses Konto kennen.

Wenn der externe E-Mail-Server so konfiguriert wurde, dass er eine moderne Authentifizierung (Microsoft OAuth 2.0 tokenbasierte Autorisierung) verwendet, wie im Fall von Exchange Online, stellen Sie sicher, dass:

- In Microsoft Azure Active Directory (Azure AD) eine Anwendung mit den erforderlichen Berechtigungen registriert wurde, damit Ihr OpenScape Business-System E-Mails versenden kann.
- Sie die Anwendungs- (Client-)ID und die Verzeichnis- (Mandanten-)ID der registrierten Anwendung kennen.

Bitten Sie Ihren Azure AD-Administrator, diese Werte bei Bedarf bereitzustellen.

- Die E-Mail-Adresse, die als Absender der E-Mails angezeigt wird, gehört zum selben Azure AD oder Mandanten wie die registrierte Anwendung.

Sie befinden sich im Fenster **E-Mail-Weiterleitung ändern** im Assistenten für die **Grundinstallation**.

Abbildung 23: Optionen für die E-Mail-Weiterleitung bei Auswahl der einfachen Authentifizierungsmethode

Schritt für Schritt

- 1) Geben Sie den **Postausgangs-Server (SMTP)** für den E-Mail-Server ein, der für den E-Mail-Versand genutzt werden soll, z. B. `smtp.web.de`. Erfragen Sie den Postausgangs-Server ggf. bei Ihrem E-Mail-Provider.

Anmerkung: Achten Sie darauf, dass der Name des Postausgangs-Servers aufgelöst werden kann. Falls nicht, müssen Sie den Assistenten für den E-Mail-Versand starten über **Service-Center > Email-Weiterleitung** und anstelle des Namens des Postausgangsservers dessen IP-Adresse eingeben.

- 2) Geben Sie den **Postausgangs-Server-Port (SMTP)** für den E-Mail-Server ein, der für den E-Mail-Versand genutzt werden soll. Erfragen Sie den Postausgangs-Server ggf. bei Ihrem E-Mail-Provider.
- 3) Wenn eine sichere Verbindung erforderlich ist, aktivieren Sie das Kontrollkästchen **Dieser Server benötigt eine verschlüsselte Verbindung (TLS/SSL)**. Erfragen Sie ggf. bei Ihrem E-Mail-Provider, ob diese Option aktiviert werden muss.
- 4) Wenn der externe E-Mail-Server für die Verwendung der einfachen Authentifizierung konfiguriert wurde, gehen Sie wie folgt vor:
 - a) Wählen Sie in der Dropdown-Liste **Authentifizierungsmethode** die Option **Einfach**.
 - b) Geben Sie den **Benutzernamen** des E-Mail-Kontos ein z. B. `max.mustermann`.
 - c) Geben Sie unter **Kennwort** und **Kennwort wiederholen** das Kennwort des E-Mail-Kontos ein.
- 5) Wenn der externe E-Mail-Server so konfiguriert wurde, dass er eine moderne Authentifizierung verwendet, gehen Sie wie folgt vor:
 - a) Wählen Sie in der Dropdown-Liste **Authentifizierungsmethode** die Option **Microsoft OAuth 2.0**.
 - b) Geben Sie die Anwendungs- (Client-)ID, die Sie vom Microsoft Azure-Portal erhalten haben, in das Feld **Anwendungs-ID** ein.
 - c) Geben Sie in das Feld **Mandant** die Verzeichnis- (Mandanten-)ID ein, die Sie vom Microsoft Azure-Portal erhalten haben.
- 6) Geben Sie die **E-Mail-Adresse** ein, die als Absender der E-Mails erscheinen soll, z. B.: `john.doe@web.de`.
- 7) Geben Sie die **E-Mail-Adresse 1** ein, um eine Benachrichtigungs-E-Mail zu erhalten, wenn die ALI-Toleranz verwendet wurde. Sie können auch eine zweite E-Mail-Adresse in das Feld **E-Mail-Adresse 2** eingeben.
- 8) Geben Sie im Feld **Empfänger für Notfälle** die E-Mail-Adresse eines Sicherheitsbeauftragten vor Ort, an den eine E-Mail gesendet wird, wenn eine Notrufnummer gewählt wird.

Der Betreff der E-Mail lautet „Neuer Notruf“. Wenn dies konfiguriert wurde, sind die Rufnummer und der Name des Anrufers, die aus der Datenbank des Systems abgerufen werden, in der E-Mail enthalten.

- 9) Wenn Sie **Microsoft OAuth 2.0** als Authentifizierungsmethode ausgewählt haben, gehen Sie wie folgt vor:
- a) Klicken Sie auf **OK & Weiter**.
 - b) Warten Sie, bis ein Autorisierungslink und ein Benutzercode erscheinen.
Der Autorisierungscode läuft nach einigen Minuten ab.
 - c) Öffnen Sie den Autorisierungslink und geben Sie den Benutzercode in das Pop-up-Fenster ein.
 - d) Melden Sie sich mit der E-Mail-Adresse an, die Sie in Schritt 6 auf Seite 248 (**E-Mail-Adresse**) eingegeben haben.
Die E-Mail-Adresse muss sich im selben Azure AD oder Mandanten befinden wie die registrierte Anwendung.
 - e) Nach erfolgreicher Authentifizierung zeigt das Pop-up-Fenster eine Meldung wie unten an:


```
Sie haben sich auf Ihrem Gerät bei <application-name>
angemeldet. Sie können dieses Fenster nun schließen.
```
 - f) Schließen Sie das Pop-up und kehren Sie zum WBM zurück.
Wenn die Authentifizierung erfolgreich war, wird die Meldung `Die Authentifizierung war erfolgreich!` angezeigt.
- 10) Falls Sie die eingegebenen E-Mail-Einstellungen überprüfen wollen, gehen Sie folgendermaßen vor:
- a) Klicken Sie auf **E-Mail-Weiterleitung testen**.
 - b) Geben Sie unter **Senden an E-Mail-Adresse** die E-Mail-Adresse eines E-Mail-Postfachs ein, auf das Sie Zugriff haben. An diese E-Mail-Adresse wird die Test-E-Mail geschickt.
 - c) Geben Sie unter **Betreff in der E-Mail** einen beschreibenden Text ein, um die E-Mail in Ihrem E-Mail-Postfach identifizieren zu können.
 - d) Klicken Sie auf **Testmail senden**. Die E-Mail-Einstellungen werden überprüft und die E-Mail an das angegebene E-Mail-Postfach gesendet.
 - e) Überprüfen Sie, ob die E-Mail in Ihrem E-Mail-Postfach angekommen ist.
 - f) War der E-Mail-Versand erfolgreich, klicken Sie auf **Zurück** und gehen Sie zum nächsten Schritt.
 - g) War der E-Mail-Versand nicht erfolgreich, klicken Sie auf **Zurück** und überprüfen nochmal Ihre E-Mail-Einstellungen.
- 11) Klicken Sie auf **OK & Weiter** und anschließend auf **Beenden**. Die Basisinstallation ist beendet. Bevor Sie die im Wizard erwähnte Datensicherung durchführen, sollten Sie die Lizenzen aktivieren.

9.8 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 in der *Administrator-Dokumentation, 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.

9.8.1 Wie Sie die Lizenzen aktivieren und zuordnen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Sie kennen den LAC (Lizenz-Autorisierungscode) für die Lizenzfreischaltung und haben eine Benutzerkennung und ein Passwort für den Zugang zum Lizenzserver.

Für die Verbindung zum Lizenzserver ist ein Internet-Zugang nötig.

Schritt für Schritt

- 1) Lizenzen online aktivieren:
 - a) Klicken Sie in der Navigationsleiste auf **Einrichtung**.
 - b) Klicken Sie im Navigationsbaum auf **Wizards > Grundinstallation**.
 - c) Klicken Sie auf **Bearbeiten**, um den Wizard **Lizenzierung** zu starten.

Setup - Wizards - Basic Installation - Licensing

Activate License Online

Licenses with Locking ID: 00-1a-e8-5d-37-81

License Authorization Code (LAC)

I have the user name and password for the License Server and want to log on.

User name

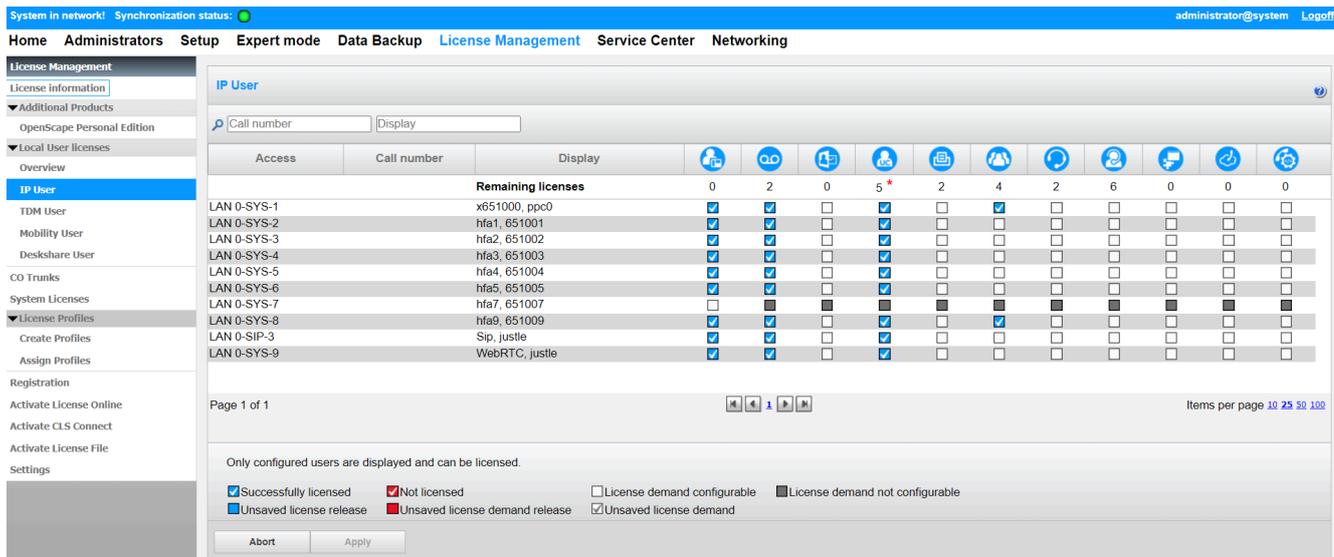
Password

Note: The response from the License Server can take up to 90 seconds !

Please enter the [registration data](#) first. Only then can the license file be activated.

- d) Geben Sie im Feld **Lizenz Autorisierungs Code (LAC)** den LAC ein.
- e) Aktivieren Sie das Kontrollkästchen **Ich habe Benutzernamen und Passwort für den Lizenzserver und möchte mich anmelden**.
- f) Geben Sie **Benutzername** und **Passwort** für die Anmeldung am Lizenzserver ein.
- g) Klicken Sie auf **OK & Weiter**. Die Verbindung zum Lizenzserver wird hergestellt und die Lizenzen freigeschaltet.

- 2) Lizenzen den Teilnehmern zuordnen:
 - a) Klicken Sie in der Navigationsleiste auf **Lizenzverwaltung**.
 - b) Navigieren Sie im Navigationsbaum unter **Lokale Benutzerlizenzen** > ... zum gewünschten Teilnehmer-Typ. Es wird Ihnen eine Liste aller Teilnehmer des ausgewählten Teilnehmer-Typs angezeigt.
 - c) Aktivieren Sie in der Zeile des gewünschten Teilnehmers das Kontrollkästchen in der Spalte **Benutzer-Lizenz** (erste Spalte mit Kontrollkästchen).



- d) Aktivieren Sie in der Zeile des gewünschten Teilnehmers die User-orientierten Lizenzen, indem Sie die gewünschten Kontrollkästchen aktivieren.

Anmerkung: User-orientierte Lizenzen können einem Teilnehmer nur zugewiesen werden, wenn dem Teilnehmer zuvor eine Teilnehmer-Lizenz (Benutzer-Lizenz) zugeordnet wurde (Schritt c).

- e) Klicken Sie auf **OK & Weiter**. Es wird geprüft, ob für Ihre Zuordnung genügend Lizenzen vorhanden sind.
Sind ausreichend Lizenzen vorhanden ist die Lizenzierung der Teilnehmer beendet.
- f) Fehlen Lizenzen, werden Ihnen die Fehler mit rot hinterlegten Kontrollkästchen angezeigt. Korrigieren Sie diese Fehler und wiederholen Sie Schritt e.

- 3) Lizenzen den Leitungen zuordnen:
 - a) Klicken Sie im Navigationsbaum auf **Amtsleitungen**. Im Bereich **Amtsleitungen** wird Ihnen die Anzahl der erworbenen Leitungslizenzen angezeigt.
 - b) Für SIP-Leitungen: Geben Sie im Bereich **Bedarf an Lizenzen für gleichzeitige Internet-Anrufe in diesem Knoten** die Anzahl der

Internet-Gespräche an, die gleichzeitig über einen ITSP geführt werden können.

- c) Für S_{2M}-Leitungen: Wählen Sie im Bereich **S2M** in der Zeile des gewünschten Slots in der Aufklappliste der Spalte **Demands** die Anzahl der gewünschten B-Kanäle aus.
- d) Für T1-Leitungen (nur USA): Wählen Sie im Bereich **T1** in der Zeile des gewünschten Slots in der Aufklappliste der Spalte **Demands** die Anzahl der gewünschten B-Kanäle aus.
- e) Klicken Sie auf **OK & Weiter**.

Anmerkung: Die Anzahl der lizenzierten SIP- und S_{2M}/T1-Leitungen darf die Anzahl der erworbenen Leitungslizenzen nicht überschreiten.

9.8.2 Wie Sie den UC Smart Client zur Installation bereitstellen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Die Hard- und Software für die Nutzung von UC Smart ist vorhanden.

Anmerkung: Für die Nutzung des UC Smart Clients myPortal Smart sind Lizenzen nötig.

Schritt für Schritt

- 1) Klicken Sie in der Navigationsleiste auf **Service-Center**.
- 2) Klicken Sie im Navigationsbaum auf **Software**.
- 3) Klicken Sie auf das Download-Symbol von **myPortal Smart** und speichern Sie die Installationsdatei auf einem freigegebenen Netz-Laufwerk.
- 4) Klicken Sie auf das Link-Symbol von **Adobe AIR** und laden Sie die Installationsdatei auf ein freigegebenes Netz-Laufwerk herunter.
- 5) Senden Sie den Benutzern von myPortal Smart die beiden Installationsdateien.
- 6) Alternativ können Sie den Benutzern von myPortal Smart auch zwei Links zuschicken, über die sie direkt auf die Installationsdateien zugreifen können:

`https://<IP-Adresse des Kommunikationssystems>/management/downloads/SmartClient.air`

`http://www.adobe.com/air`

9.8.3 Wie Sie die UC Suite Clients zur Installation bereitstellen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Die Hard- und Software für die Nutzung von UC Suite ist vorhanden.

Anmerkung: Für die Nutzung der UC Suite Clients sind Lizenzen nötig.

Schritt für Schritt

- 1) Damit die Installationsdateien einem Teilnehmer automatisch zur Verfügung gestellt werden können, vergewissern Sie sich, ob folgende Schritte durchgeführt worden sind:
 - a) Die E-Mail-Adressen der Teilnehmer müssen entweder zusammen mit den Teilnehmerdaten über eine XML-Datei importiert worden sein oder eingetragen werden unter **Einrichtung > UC Suite > Benutzerverzeichnis**.
 - b) Ein Mail-Server muss eingetragen sein.

Anmerkung: Einen E-Mail-Server können Sie auch nachträglich eintragen unter **Service-Center > E-Mail-Weiterleitung**.

Alle Teilnehmer, deren E-Mail-Adressen bekannt sind, erhalten eine E-Mail mit dem Link auf das Installationsverzeichnis der UC Clients und mit einer Erste-Schritte-Anleitung. Im Installationsverzeichnis liegt zusätzlich eine Readme-Datei mit Informationen zur Installation der Software auf den Client-PCs.

- 2) Falls die nötigen Schritte für eine automatische Benachrichtigung nicht erfüllt sind, können Sie die Installationsdateien auch manuell zur Verfügung stellen. Gehen Sie dazu folgendermaßen vor:
 - a) Klicken Sie in der Navigationsleiste auf **Service-Center**.
 - b) Klicken Sie im Navigationsbaum auf **Software**.
 - c) Klicken Sie auf den gewünschten UC Client und speichern Sie die gezippte Installationsdatei auf einem freigegebenen Netz-Laufwerk.
 - d) Klicken Sie im Navigationsbaum auf **Dokumente** und wählen Sie die Aufklappliste **Bedienungsanleitung**.
 - e) Klicken Sie auf die Dokumentation zum gewünschten UC Client und speichern Sie die Dokumentationsdatei auf einem freigegebenen Netz-Laufwerk.
 - f) Senden Sie den Benutzern der UC Clients die gezippte Installationsdatei und die Dokumentationsdatei per E-Mail oder teilen Sie den Benutzern den Ablageort der Dateien mit.
 - g) In der Zip-Datei mit den Installationsdateien ist auch eine Readme-Datei enthalten. Weisen Sie die Benutzer darauf hin, dass die Installation der UC Clients anhand der Installationshinweise in der Readme-Datei durchgeführt werden muss.
- 3) Alternativ können Sie den UC Benutzern auch Links zuschicken, über die sie direkt auf die Installationsdateien der UC Clients zugreifen können.
 - a) Klicken Sie in der Navigationsleiste auf **Service-Center**.
 - b) Klicken Sie im Navigationsbaum auf **Software**.
 - c) Klicken Sie auf die Schaltfläche **Applikationslinks anzeigen**. Es werden Ihnen mehrere Links angezeigt, abhängig vom verwendeten Betriebssystem und vom gewünschten UC Client. Zum Beispiel:

```
https://<IP-Adresse des Kommunikationssystems>/  
management/downloads/install-common.zip
```

9.8.4 Wie Sie eine Datensicherung durchführen

Voraussetzungen

Sie sind am WBM mit dem Profil **Advanced** angemeldet.

Für eine Datensicherung auf einem USB-Medium (USB-Stick oder USB-Festplatte) muss das USB-Medium an der USB-Server-Schnittstelle angeschlossen sein.

Anmerkung: Weitere Informationen zur Datensicherung siehe *Administratordokumentation, Sofortiges Sichern*.

Schritt für Schritt

- 1) Klicken Sie in der Navigationsleiste auf **Datensicherung**.
- 2) Klicken Sie im Navigationsbaum auf **Backup - sofort**.
- 3) Geben Sie im Bereich **Name** im Feld **Kommentar** einen Kommentar für das Backup-Set ein, um das Backup-Set bei einer möglichen Wiederherstellung leichter identifizieren zu können. Vermeiden Sie bei der Eingabe Umlaute und Sonderzeichen.
- 4) Aktivieren Sie im Bereich **Geräte** das Ziellaufwerk, auf dem das Backup-Set gespeichert werden soll.
- 5) Klicken Sie auf **OK & Weiter**. In einem weiteren Fenster wird Ihnen der Fortschritt der Sicherung angezeigt.
- 6) Die Sicherung ist erfolgreich, wenn die Meldung **Sicherung erfolgreich ausgeführt!** erscheint. Klicken Sie auf **Beenden**.
- 7) Wenn Sie als Backup-Medium einen USB-Stick verwenden, warten Sie ab, bis die LED des USB-Sticks aufhört zu blinken. Erst dann ist die Sicherung erfolgreich auf dem USB-Stick gespeichert. Entfernen Sie anschließend den USB-Stick.
- 8) Die Erstinbetriebnahme mit dem WBM ist nun abgeschlossen. Beenden Sie das WBM, indem Sie rechts oben auf den Link **Abmelden** klicken und anschließend das Fenster schließen.

Anmerkung: Falls eine neue Software-Version für das Kommunikationssystem vorliegt, wird Ihnen das auf der Startseite des WBM mitgeteilt - vorausgesetzt der Internet-Anschluss ist korrekt eingerichtet. Liegt eine neue Software-Version vor, führen Sie ein Update durch (siehe *Administratordokumentation, Update des Kommunikationssystems*).

9.9 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.

9.9.1 Wie Sie ein IP-Telefon konfigurieren**Voraussetzungen**

Das IP-Telefon ist an das interne Netz angeschlossen und betriebsbereit.

Anmerkung: Hier wird die Konfiguration am Beispiel eines OpenStage 40/60/80 IP-Systemtelefons beschrieben. Für ein anderes IP-Telefon müssen diese Einstellungen analog durchgeführt werden. Sehen Sie dazu bitte in der Anleitung Ihres IP-Telefons nach.

Schritt für Schritt

- 1) Um in den Administrationsmodus des IP-Systemtelefons zu gelangen, drücken Sie am Telefon die Taste für das Einstellungen-/Anwendungen-Menü.
- 2) Blättern Sie im Register `Einstellungen` bis `Admin` und bestätigen Sie mit der OK-Taste.
- 3) Geben Sie das Administrator-Passwort (Standard: `123456`) ein und bestätigen Sie mit der OK-Taste.
- 4) Wenn Sie im internen Netz den DHCP-Server des Kommunikationssystems verwenden, überspringen Sie den nächsten Schritt.
- 5) Wenn Sie im internen Netz nicht den DHCP-Server des Kommunikationssystems verwenden, müssen Sie die IP-Adresse des Deployment Servers (DLS) und des Kommunikationssystems eingeben, damit die Software des IP-Systemtelefons automatisch aktualisiert werden kann. Das gilt nur für IP-Systemtelefone. Gehen Sie folgendermaßen vor:
 - a) Blättern Sie bis `Network` und bestätigen Sie mit der OK-Taste.
 - b) Blättern Sie bis `Update service (DLS)` und bestätigen Sie mit der OK-Taste.
 - c) Blättern Sie bis `DLS address` und bestätigen Sie mit der OK-Taste.
 - d) Geben Sie als Deployment Server die IP-Adresse des Kommunikationssystems (Standard: `192.168.1.2`) an und bestätigen Sie mit der OK-Taste.
 - e) Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.
 - f) Blättern Sie bis `IPv4 configuration` und bestätigen Sie mit der OK-Taste.
 - g) Blättern Sie bis `Route (default)` und bestätigen Sie mit der OK-Taste.
 - h) Geben Sie die IP-Adresse des Kommunikationssystems (Standard: `192.168.1.2`) an und bestätigen Sie mit der OK-Taste.

- i) Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.
- j) Navigieren Sie eine Menüebene zurück mit der Zurück-Taste.
- 6) Legen Sie die Rufnummer des Telefons fest:
 - a) Blättern Sie bis `System` und bestätigen Sie mit der OK-Taste.
 - b) Blättern Sie bis `Identity` und bestätigen Sie mit der OK-Taste.
 - c) Blättern Sie bis `Terminal number` und bestätigen Sie mit der OK-Taste.
 - d) Geben Sie die festgelegte Rufnummer ein (z.B. 120) und bestätigen Sie mit der OK-Taste.
 - e) Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.
- 7) Navigieren Sie eine Menüebene zurück mit der Zurück-Taste.
- 8) Wenn das Systemtelefon bedingt durch die Änderungen einen Neustart durchführen muss, erscheint in dem Menü `Admin` der Menüpunkt `Restart`. Bestätigen Sie `Restart` mit der OK-Taste und anschließend `Yes` ebenso mit der OK-Taste. Das Systemtelefon führt einen Neustart durch und meldet sich am Kommunikationssystem an.

9.9.2 Wie Sie ein SIP-Telefon konfigurieren

Voraussetzungen

Das SIP-Telefon ist an das Kunden-LAN angeschlossen und betriebsbereit.

Anmerkung: Hier wird die Konfiguration am Beispiel eines OpenStage 40/60/80 SIP-Systemtelefons beschrieben. Für ein anderes SIP-Telefon müssen diese Einstellungen analog durchgeführt werden. Sehen Sie dazu bitte in der Anleitung Ihres SIP-Telefons nach.

Schritt für Schritt

- 1) Um in den Administrationsmodus des SIP-Systemtelefons zu gelangen, drücken Sie am Telefon die Taste für das Einstellungen-/Anwendungen-Menü.
- 2) Blättern Sie im Register `Einstellungen` bis `Administrator (Admin)` und bestätigen Sie mit der OK-Taste.
- 3) Geben Sie das Administrator-Passwort (Standard: 123456) ein und bestätigen Sie mit der OK-Taste.
- 4) Wenn Sie im internen Netz den DHCP-Server des Kommunikationssystems verwenden, überspringen Sie den nächsten Schritt.
- 5) Wenn Sie im internen Netz nicht den DHCP-Server des Kommunikationssystems verwenden, müssen Sie die IP-Adresse des Deployment Servers (DLS) und des Kommunikationssystems eingeben, damit die Software des SIP-Systemtelefons automatisch aktualisiert werden kann. Das gilt nur für SIP-Systemtelefone. Gehen Sie folgendermaßen vor:
 - a) Blättern Sie bis `Network` und bestätigen Sie mit der OK-Taste.
 - b) Blättern Sie bis `Update service (DLS)` und bestätigen Sie mit der OK-Taste.
 - c) Blättern Sie bis `DLS address` und bestätigen Sie mit der OK-Taste.

- d) Geben Sie als Deployment Server die IP-Adresse des Kommunikationssystems (Standard: 192.168.1.2) an und bestätigen Sie mit der OK-Taste.
 - e) Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.
 - f) Blättern Sie bis `IPv4 configuration` und bestätigen Sie mit der OK-Taste.
 - g) Blättern Sie bis `Route (default)` und bestätigen Sie mit der OK-Taste.
 - h) Geben Sie die IP-Adresse des Kommunikationssystems (Standard: 192.168.1.2) an und bestätigen Sie mit der OK-Taste.
 - i) Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.
 - j) Navigieren Sie eine Menüebene zurück mit der Zurück-Taste.
- 6) Legen Sie die SNTP-Zeiteinstellungen fest:**
- a) Blättern Sie bis `Date and time` und bestätigen Sie mit der OK-Taste.
 - b) Blättern Sie bis `Time source` und bestätigen Sie mit der OK-Taste.
 - c) Blättern Sie bis `SNTP IP address` und bestätigen Sie mit der OK-Taste.
 - d) Geben Sie die IP-Adresse des Kommunikationssystems (Standard: 192.168.1.2) an und bestätigen Sie mit der OK-Taste.
 - e) Blättern Sie bis `Timezone offset` und bestätigen Sie mit der OK-Taste.
 - f) Geben Sie die Abweichung der lokalen Uhrzeit von der UTC-Zeit (Universal Time Coordinated) in Stunden an (Deutschland: 1) und bestätigen Sie mit der OK-Taste.
 - g) Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.
 - h) Navigieren Sie eine Menüebene zurück mit der Zurück-Taste.
- 7) Legen Sie die Rufnummer des Telefons fest:**
- a) Blättern Sie bis `System` und bestätigen Sie mit der OK-Taste.
 - b) Blättern Sie bis `Identity` und bestätigen Sie mit der OK-Taste.
 - c) Blättern Sie bis `Terminal number` und bestätigen Sie mit der OK-Taste.
 - d) Geben Sie die festgelegte Rufnummer ein (z.B. 120) und bestätigen Sie mit der OK-Taste.
 - e) Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.
- 8) Legen Sie die SIP-Authentifizierungsdaten fest:**
- a) Blättern Sie bis `Registration` und bestätigen Sie mit der OK-Taste.
 - b) Blättern Sie bis `SIP session` und bestätigen Sie mit der OK-Taste.
 - c) Notieren Sie sich die `Realm` oder geben Sie bei Bedarf eine neue `Realm` (z.B. OSBIZ-SIP) ein.
 - d) Notieren Sie sich die `User ID` oder geben Sie bei Bedarf eine neue `User ID` (z.B. SIP-120) ein.
 - e) Vergeben Sie ein `Password` für die Registrierung am SIP Server.
 - f) Blättern Sie bis `Save & Exit` und bestätigen Sie mit der OK-Taste.
- 9) Navigieren Sie mit der Zurück-Taste zum Menü `Admin` zurück.**
- 10) Wenn das Systemtelefon bedingt durch die Änderungen einen Neustart durchführen muss, erscheint in dem Menü `Admin` der Menüpunkt `Restart`. Bestätigen Sie `Restart` mit der OK-Taste und anschließend `Yes` ebenso mit der OK-Taste. Das Systemtelefon führt einen Neustart durch und meldet sich am Kommunikationssystem an.**

10 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 auf Seite 265
<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 <i>OpenScape Business Servicedokumentation, Montage der Hardware - Beschreibung der Baugruppen</i>.</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 <i>OpenScape Business Servicedokumentation, Montage der Hardware - Beschreibung der Baugruppen</i>.</p>
<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 auf Seite 191.</p>	<p>Konfiguration der UC Booster Card</p> <p>Die Konfiguration der UC Booster Card wird nachträglich an einem bereits konfigurierten OpenScape Business Kommunikationssystem X3/X5/X8 durchgeführt.</p> <p>Beschreibung siehe Integration ins Kunden-LAN auf Seite 191.</p> <p>Einzelheiten zur Konfiguration siehe Konfiguration der UC Booster Card auf Seite 267</p>

Integration in neues Kommunikationssystem	Integration in bestehendes Kommunikationssystem
<p>Basiskonfiguration</p> <p>Die Basiskonfiguration wird zusammen mit der Erstinstallation des OpenScape Business Kommunikationssystems X3/X5/X8 durchgeführt.</p> <p>Beschreibung siehe Basiskonfiguration auf Seite 202.</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 auf Seite 202.</p> <p>Für die Besonderheiten bei der Basiskonfiguration siehe Basiskonfiguration auf Seite 274</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 auf Seite 249.</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 auf Seite 249.</p> <p>Für die Besonderheiten bei den abschließenden Tätigkeiten siehe Abschließende Tätigkeiten auf Seite 274</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

Ersteinrichtung OpenScape Business UC Booster

Voraussetzungen für die Ersteinrichtung

Integration in neues Kommunikationssystem	Integration in bestehendes Kommunikationssystem
<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>
<p>Installation der Kommunikationssoftware</p>	<p>Installation der Kommunikationssoftware</p>
<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 auf Seite 191.</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 auf Seite 191.</p> <p>Einzelheiten zur Konfiguration siehe Konfiguration des UC Booster Servers auf Seite 271</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 auf Seite 202.</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 auf Seite 202.</p> <p>Für die Besonderheiten bei der Basiskonfiguration siehe Basiskonfiguration auf Seite 274</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 auf Seite 249.</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 auf Seite 249.</p> <p>Für die Besonderheiten bei den abschließenden Tätigkeiten siehe Abschließende Tätigkeiten auf Seite 274</p>

10.1 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, Gate View, Directory Services, usw.). Bei einer Integration in ein bereits lizenziertes Kommunikationssystem gibt es keine Activation Period mehr.
- Ein IP-Adressen-Schema ist vorhanden und bekannt.
- Ein Rufnummernplan ist vorhanden und bekannt.

Für UC Booster Card

Folgende Voraussetzungen sind für den Betrieb der UC Booster Card zu beachten.

- OpenScape Business-Hardware:

Die UC Booster Card ist installiert.

- Switch:

Der Switch, über den die UC Booster Card mit dem Kommunikationssystem verbunden ist, sollte IPv6-fähig sein, damit die UC Booster Card während der Ersteinrichtung eine IP-Adresse erhält.

Ist der Switch nicht IPv6-fähig, blinkt die rote LED des Kommunikationssystems. In diesem Fall muss der Admin-Port des Systems über ein zusätzliches Ethernet-Kabel mit dem zweiten LAN-Port der UC Booster Card verbunden werden. Dadurch erhält die UC Booster Card automatisch eine IPv4-IP-Adresse über das IPv6-Protokoll. Sobald die UC Booster Card über IP erreichbar ist, erlischt die rote LED des Kommunikationssystems. Anschließend kann die gewünschte IP-Adresse für die UC Booster Card während der Ersteinrichtung 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
- Microsoft Edge
- Mozilla Firefox
- Google Chrome

Die unterstützten Browserversionen finden Sie in den *Software-Versionshinweisen*. Falls 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 Mainboard und UC Booster Card 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

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 (Admin-PC).
- Microsoft Edge
- Mozilla Firefox (Linux-Server/Admin-PC)
- Google Chrome

Die erforderliche Browserversion finden Sie in den *Software-Versionshinweisen*. 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](#) auf Seite 277).

10.2 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).

10.2.1 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

Ersteinrichtung OpenScape Business UC Booster

Inbetriebnahme UC Booster Card

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.

10.3 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.

10.3.1 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.

10.3.2 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.

10.3.3 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).

10.3.3.1 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.

10.4 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.

10.4.1 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>).

10.4.1.1 Kommunikationssoftware auf einem Linux-Server oder in einer virtuellen Umgebung 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 durch Klicken auf **Continue** fortgesetzt werden. Bei schwerwiegender Unterschreitung wird die Installation automatisch abgebrochen.
- 6) Es wird untersucht, ob zusätzliche RPM-Pakete installiert werden müssen. Falls ja, bestätigen Sie dies mit **Confirm**. Später muss in diesem Fall auf die SLES 12 DVD oder die .ISO-Datei zurückgewechselt werden.
- 7) Es erscheint ein Fenster mit den Lizenzbestimmungen (EULA, End User License Agreement). Lesen Sie sich die Lizenzbestimmungen durch und akzeptieren Sie die Lizenzbestimmungen mit **Yes**.
- 8) Wenn im Kunden-LAN bereits ein DHCP-Server vorhanden ist (z.B. der DHCP-Server des Internet-Routers), brechen Sie hier die Konfiguration des Linux-DHCP-Servers mit **No** ab. Fahren Sie mit Schritt [12](#) fort.

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.

10.4.2 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.

10.4.2.1 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:
- Geben Sie im Feld **Passwort** nochmal das Standard-Passwort `administrator` ein.
 - 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.

- Klicken Sie auf **Login**.
- Wählen Sie das aktuelle Datum aus und tragen Sie die Uhrzeit korrekt ein.
- Klicken Sie auf **OK & Weiter**. Sie werden automatisch vom WBM abgemeldet.
- 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.

- Geben Sie im zweiten Feld unter **Login** Ihr neu definiertes Passwort für den Zugang als Administrator ein.
 - Klicken Sie auf **Login**. Es erscheint die Startseite des WBM.
 - Klicken Sie in der Navigationsleiste auf **Administratoren**.
 - Aktivieren Sie in der **Administratoren-Liste** das Kontrollkästchen vor dem Listeneintrag **Administrator**.
 - Klicken Sie auf **Bearbeiten**.
 - Wählen Sie in der Aufklappliste **Benutzerrolle** das Benutzerprofil **Expert** aus.
 - Klicken Sie auf **OK & Weiter**.
 - Melden Sie sich am WBM ab über den Link **Abmelden** rechts oben.
 - 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**.

10.4.3 Software-Update für die UC Booster Card

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).

10.5 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.

10.6 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.

10.7 Deinstallation der Kommunikationssoftware

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

10.7.1 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.

10.8 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 *Erstinstallation OpenScape Business UC Booster - 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 *Konfiguration OpenScape Business X3/X5/X8 - Integration ins Kunden-LAN - 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 *Konfiguration OpenScape Business X3/X5/X8 - Integration ins Kunden-LAN - 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 *Erstinstallation OpenScape Business UC Booster - Erstinbetriebnahme UC Booster Server - 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 *Erstinstallation OpenScape Business UC Booster - Erstinbetriebnahme UC Booster Server - 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 *Maintenance - Restart, Reload, Shutdown - 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 *Maintenance - Update*.

10) Wiederherstellung der Konfigurationsdaten

Spielen Sie im WBM des Kommunikationssystems die Sicherung der Konfigurationsdaten des Kommunikationssystems ein. Kommunikationssystem und Kommunikationssoftware führen anschließend einen Neustart durch. Die Verbindung zu den UC Clients ist wieder hergestellt.

Beschreibung der Datenwiederherstellung siehe *Maintenance - Sichern und Wiederherstellen - Wiederherstellen*.

10.9 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 nicht dauerhaft in der Firewall geöffnet (z.B. ist der TFTP-Port nur bei aktiviertem Gate View offen).

Beschreibung	TCP	UDP	Portnummer	OpenScape Business X	UC Booster Card	OpenScape Business S	UC Booster Server
Systemkomponenten							
Admin Portal (https)	X		443	X	X	X	X
CAR Update Registration	X		12061	X		X	
CAR Update Server	X		12063	X		X	
CLA	X		61740	O		O	O
CLA Auto Discovery		X	23232	X		X	X
Communication Client-Installationsprogramm	X		8101	X	X	X	X

Ersteinrichtung OpenScape Business UC Booster

Beschreibung	TCP	UDP	Portnummer	OpenScape Business X	UC Booster Card	OpenScape Business S	UC Booster Server
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	
Gateview	X		8000-8010		O	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
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

Beschreibung	TCP	UDP	Portnummer	OpenScape Business X	UC Booster Card	OpenScape Business S	UC Booster Server
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	
TFTP		X	69		O	O	O
VSL	X		8770-8780		X	X	X
Webadmin for Clients	X		8803	X	X	X	X
xXMPP Connection Manager	X		5262		X	X	X
XMPP Server	X		5269		X	X	X
Webbased Clients							
Webbased Clients (http)	X		8801	X	X	X	X
Webbased Clients (https)	X		8802	X	X	X	X

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.

Nicht mehr angebotene Komponenten

Hauptverteiler MDFU (optional)

11 Nicht mehr angebotene Komponenten

Dieser Abschnitt enthält Informationen zu nicht mehr angebotenen Komponenten, die hier als Referenz angegeben werden.

11.1 Hauptverteiler MDFU (optional)

Der Anschluss von Telefonen, Amtsleitungen usw. an OpenScape Business X3W und OpenScape Business X5W kann direkt an den Baugruppen der Kommunikationssysteme oder über den externen Hauptverteiler MDFU erfolgen.

Der Hauptverteiler MDFU (Main Distribution Frame Universal) stellt neun Einbauplätze für Trenn- und Rangierleisten zur Verfügung.

Abmessungen:

- Höhe: 367,0 mm
- Breite = 328,8 mm
- Tiefe = 125,4 mm

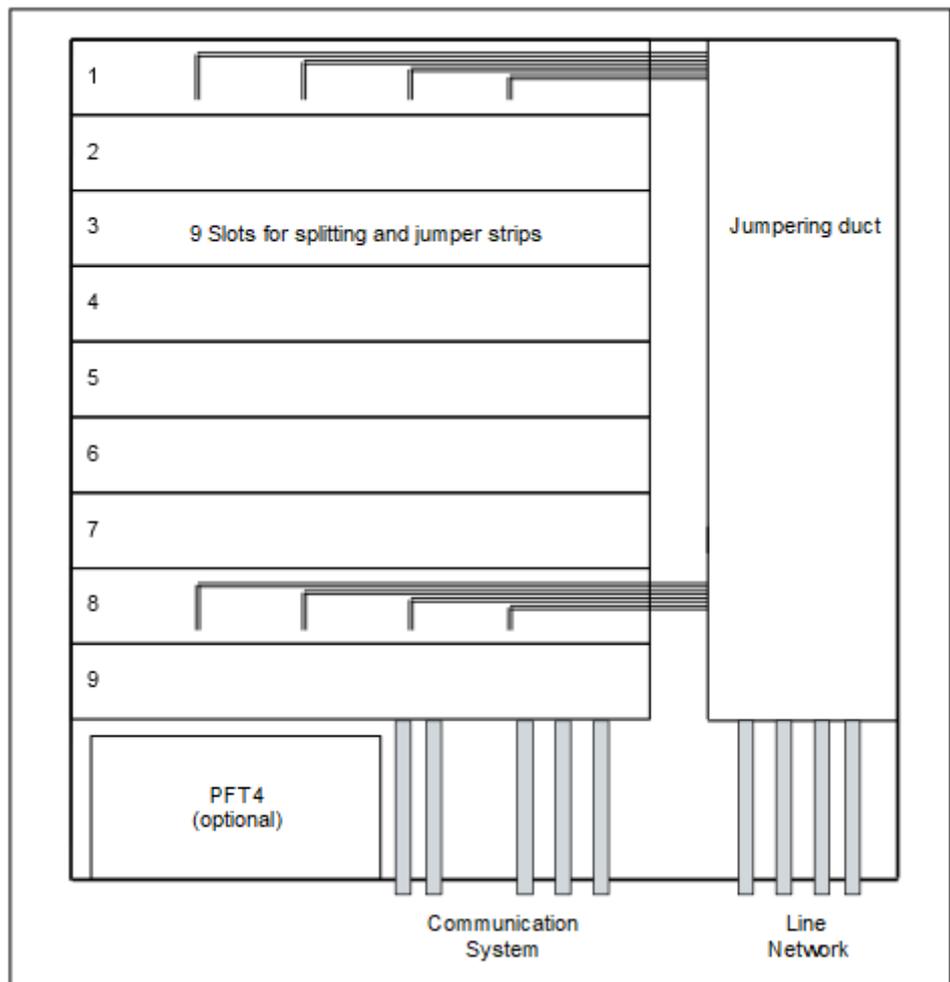


Abbildung 24: Hauptverteiler MDFU

Anmerkung: Beachten und befolgen Sie die Anweisungen des Herstellers zur Montage und Schutzerdung, falls Sie nicht den MDFU sondern den Hauptverteiler eines anderen Herstellers verwenden.

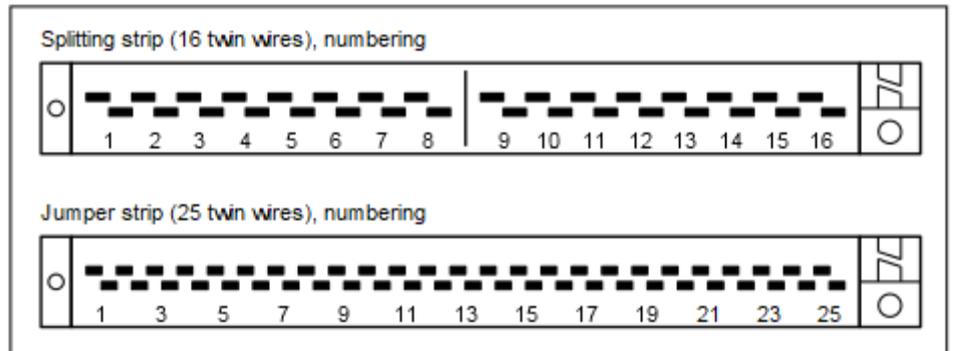


Abbildung 25: Trenn- und Rangierleiste – Nummerierung der Anschlüsse

11.1.1 Wie Sie den Hauptverteiler MDFU an einer Wand befestigen

Voraussetzungen

Eine tragfähige Wand mit ausreichend Platz für die Montage des Hauptverters MDFU steht zur Verfügung.

Schritt für Schritt

- 1) Befestigen Sie die beiliegende Bohrschablone am gewünschten Montageort.
- 2) Bohren Sie die Löcher.
- 3) Schieben Sie die Dübel in die Bohrlöcher und drehen Sie die Schrauben mit ca. 5 mm Überstand ein.
- 4) Nehmen Sie den Gehäusedeckel des MDFU ab.
- 5) Hängen Sie den MDFU an den Halterungen ein und richten Sie diesen aus.
- 6) Drehen Sie die Schrauben fest.

11.2 Verbindungskabel zum externen Hauptverteiler (optional)

Der Anschluss von Telefonen, Amtsleitungen usw. an OpenScape Business X3W und OpenScape Business X5W kann über den Hauptverteiler MDFU oder einen anderen externen Hauptverteiler erfolgen. Für die Verbindung des Kommunikationssystems mit einem Hauptverteiler stehen verschiedene Möglichkeiten zur Verfügung.

CABLU S30269-Z41-A30

CABLU (24 DA) mit

Nicht mehr angebotene Komponenten

- sechs Wieland-Schraubklemmen für den direkten Anschluss an die Randstecker der Baugruppen der Kommunikationssysteme OpenScape Business X3W und OpenScape Business X5W
- Rangierleiste zur Montage im MDFU

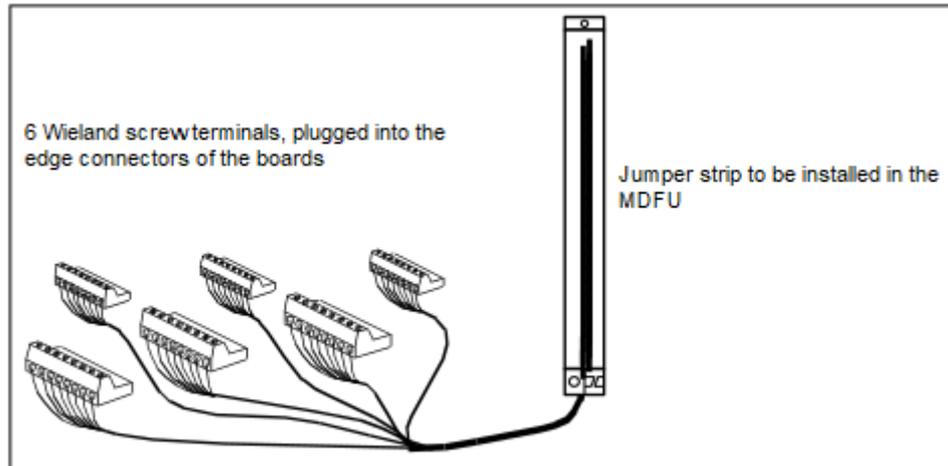


Abbildung 26: CABLU S30269-Z41-A30

Open-End-Kabel S30267-Z322-Axxx

Open-End-Kabel (24 DA) mit sechs Wieland-Schraubklemmen für den direkten Anschluss an die Randstecker der Baugruppen der Kommunikationssysteme OpenScape Business X3W und OpenScape Business X5W. Das Kabel muss manuell auf eine Trenn- oder Rangierleiste im MDFU oder einem anderen externen Hauptverteiler aufgelegt werden.

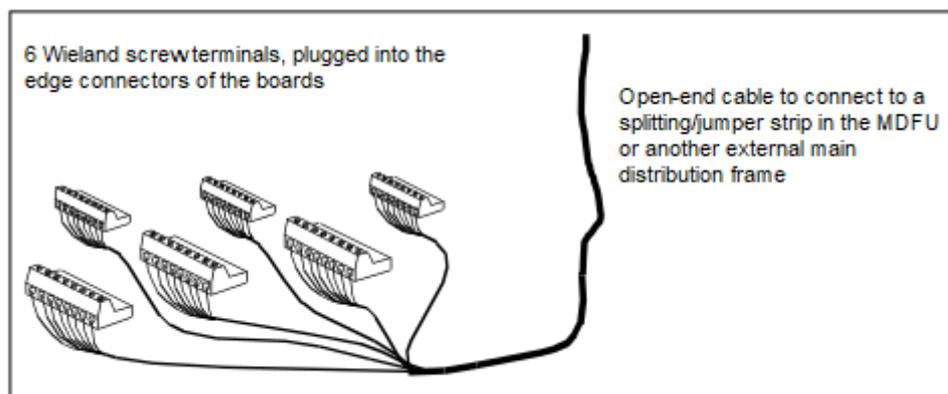


Abbildung 27: Open-End-Kabel S30267-Z322-Axxx

CABLU S30269-Z100-A11/-A21

CABLU (16 DA) mit

- einer SIPAC 1 SU-Buchse zum Anschluss an den Backplane-Stecker X8 des Kommunikationssystems OpenScape Business X5W
- Trennleiste zur Montage im MDFU

CABLU S30269-Z100-A14/-A24

CABLU (24 DA) mit

- zwei SIPAC 1 SU-Buchsen zum Anschluss an die Backplane-Stecker X8 und X9 des Kommunikationssystems OpenScape Business X5W
- Rangierleiste zur Montage im MDFU

CABLU S30267-Z346-A30

CABLU mit

- einer SIPAC 1 SU-Buchse zum Anschluss an den Backplane-Stecker X8 des Kommunikationssystems OpenScape Business X5W
- CHAMP-Stecker zum Anschluss eines externen Hauptverteilers

CABLU S30267-Z365-A30

CABLU mit

- zwei SIPAC 1 SU-Buchsen zum Anschluss an die Backplane-Stecker X8 und X9 des Kommunikationssystems OpenScape Business X5W
- CHAMP-Stecker zum Anschluss eines externen Hauptverteilers

11.2.1 So schließen Sie ein Verbindungskabel am externen Hauptverteiler an (optional)

Voraussetzungen



Achtung:

Elektrischer Schlag durch Berühren spannungsführender Leitungen

Schutzerden Sie Ihr Kommunikationssystem und alle verwendeten Hauptverteiler vor Anschluss der Telefone und Leitungen durch separate Schutzleiter.

Die Gehäusekappe des Kommunikationssystems ist nicht montiert.

Schritt für Schritt

1) Wählen Sie das geeignete Verbindungskabel je nach Kommunikationssystem und Baugruppe.

Wenn		Dann
Kommunikationssystem	Baugruppe	Verbindungskabel
OpenScape Business X3W	Alle Peripheriebaugruppen und die Mainboards OCCM, OCCMA und OCCMB	<p>Anschluss an den externen MDF: CABLU mit sechs Wieland-Schraubklemmen (zum direkten Anschluss an den Randsteckern der Baugruppen) und Rangierleiste für 24 DA:</p> <ul style="list-style-type: none"> • S30269-Z41-A30: 3 m Länge <p>Anschluss an den MDFU oder an einem anderen externen Hauptverteiler: Open-End-Kabel (24 DA) mit sechs Wieland-Schraubklemmen (zum direkten Anschluss an den Randsteckern der Baugruppen):</p> <ul style="list-style-type: none"> • S30267-Z322-A100: 10 m Länge
OpenScape Business X5W	Alle Peripheriebaugruppen (außer den Peripheriebaugruppen im SIPAC-Format) und die Mainboards OCCM, OCCMA und OCCMB	<p>Anschluss an den MDFU: CABLU mit sechs Wieland-Schraubklemmen (zum direkten Anschluss an den Randsteckern der Baugruppen) und Rangierleiste für 24 DA:</p> <ul style="list-style-type: none"> • S30269-Z41-A30: 3 m Länge <p>Anschluss an den MDFU oder an einem anderen externen Hauptverteiler: Open-End-Kabel (24 DA) mit sechs Wieland-Schraubklemmen (zum direkten Anschluss an den Randsteckern der Baugruppen):</p> <ul style="list-style-type: none"> • S30267-Z322-A100: 10 m Länge

2) Wählen Sie eine der folgenden Konnektivitätsoptionen für das Kommunikationssystem aus:

- Wenn Sie eine CABLU mit sechs Wieland-Schraubklemmen verwenden, befestigen Sie die Schraubklemmen an den gewünschten Randsteckern der gewünschten Baugruppen.
- Wenn Sie eine CABLU mit einer SIPAC 1 SU-Buchse verwenden, verbinden Sie das Kabel mit dem Backplane-Anschluss X8.

3) Befestigen Sie das Verbindungskabel mit Kabelbindern am Kommunikationssystem.

4) Wählen Sie eine der folgenden Optionen zum Anschluss des MDFU oder eines anderen externen Hauptverteilers:

- Wenn Sie den MDFU und eine CABLU mit einer Trennleiste oder einer Rangierleiste verwenden, installieren Sie die Leiste im MDFU.

Informationen zu den Hauptmerkmalen des MDFU und zur Nummerierung der Trenn- und Rangierleisten finden Sie unter [Hauptverteiler MDFU \(optional\)](#).

- Wenn Sie den MDFU und ein Open-End-Kabel verwenden, schließen Sie das Kabel an die gewünschte Trenn-/Rangierleiste im MDFU an.

Vorgehensweise:

Freilegen der Kabelleiter.

Ziehen Sie den Kabelmantel auf einer Länge von ca. 3 cm ab. Schneiden Sie den Kontakteiter auf ca. 2,5 cm und fixieren Sie ihn mit Klebeband am Kabelmantel (mindestens 1,5 Mal umwickeln).

Verwenden Sie ein Standardverdrahtungswerkzeug zum Verlegen der Kabelleiter.

Tabelle 8: Farbcodes für die Open-End-Kabel

Farbgruppe	Paar	a-Ader	b-Ader
1	1	weiß/blau	blau/weiß
		weiß/orange	orange/weiß
	2	weiß/grün	grün/weiß
		weiß/braun	braun/weiß
	3	weiß/grau	grau/weiß
		rot/blau	blau/rot
2	4	rot/orange	orange/rot
		rot/grün	grün/rot
	5	rot/braun	braun/rot
		rot/grau	grau/rot
	6	schwarz/blau	
		schwarz/orange	
3	schwarz/grün		
	schwarz/braun		

Nicht mehr angebotene Komponenten

Farbgruppe	Paar	a-Ader	b-Ader
	12	schwarz/orange	blau/schwarz
			orange/schwarz
	13	schwarz/grün	grün/schwarz
	14	schwarz/braun	braun/schwarz
	15	schwarz/grau	grau/schwarz
4	16	gelb/blau	blau/gelb
	17	gelb/orange	orange/gelb
	18	gelb/grün	grün/gelb
	19	gelb/braun	braun/gelb
20	gelb/grau	grau/gelb	
5	21	violett/blau	blau/violett
	22	violett/orange	orange/violett
	23	violett/grün	grün/violett
24	violett/braun	braun/violett	

Informationen zu den Hauptmerkmalen des MDFU und zur Nummerierung der Trenn- und Rangierleisten finden Sie unter [Hauptverteiler MDFU \(optional\)](#).

- Setzen Sie bei Verwendung eines externen Hauptverteilers mit CHAMP-Anschlüssen den Stecker in die gewünschte CHAMP-Buchse des externen Hauptverteilers ein.
 - Schließen Sie bei Verwendung eines anderen externen Hauptverteilers und eines Open-End-Kabels das Kabel an die gewünschte Trenn-/Rangierleiste im externen Hauptverteiler an.
- 5) Befestigen Sie das Verbindungskabel mit Kabelbindern am MDFU oder am externen Hauptverteiler.

Index

Sonderzeichen

§§Komponenten auspacken [36](#)

A

Abschirmblende für Baugruppe [88](#)
 Abschirmkappe für Baugruppe [131](#)
 Anschluss- oder Abschirm-Panel [135](#)
 Anschlussbereich
 OpenScape Business S [24](#)
 OpenScape Business UC Booster Server [24](#)

B

Baugruppen-Initialisierung [125](#)
 Baugruppeninstallation
 OpenScape Business X3R und X5R [87](#)
 OpenScape Business X3W und X5W [52](#)
 OpenScape Business X8 [129](#)
 Bestimmungsgemäßer Gebrauch der
 Kommunikationssysteme und Server [22](#)
 Betriebsbedingungen (klimatisch, mechanisch)
 OpenScape Business S [30](#)
 OpenScape Business UC Booster Server [30](#)
 OpenScape Business X3, X5, X8 [29](#)
 Blitzschutzanforderungen [26](#)
 Brandschutzanforderungen [25](#)

C

CE-Kennzeichnung [26](#)
 CE-Konformität [28](#)

D

Darstellungskonventionen [12](#)
 Datenschutz [27](#)
 Datensicherheit [27](#)

E

Entsorgung [23](#)

F

Funkstörung [27](#)

H

Handlungsanweisung [12](#)
 Hauptverteiler MDFU [280](#)
 Hauptverteiler MDFU-E
 Schutzerdung [113](#)

Hauptverteiler MDFU:Wandmontage [281](#)

I

Installation [182](#), [260](#)
 Internet-Telefonie-Service-Provider (ITSP) [224](#)
 IP-Adressen-Schema [186](#)

J

Java Runtime Environment (JRE) [183](#)

K

Konformität
 internationale Normen [29](#)
 US- und kanadische Normen [28](#)
 Konzept [12](#)

L

Lizenzserver (CLS)
 IP-Adresse ändern [252](#)

M

MDFU [280](#)
 Schutzerdung [41](#)
 MDFU-E
 Schutzerdung [113](#)
 MDFU:Wandmontage [281](#)

O

OpenScape Business X3R
 Baugruppeninstallation [87](#)
 OpenScape Business X3R
 19"-Schrankmontage [73](#)
 Abschirmblende für Baugruppe [88](#)
 Montage [73](#)
 Montagestandort [32](#)
 OpenScape Business X3R: Anschluss von Telefonen und
 Geräten [92](#)
 OpenScape Business X3R:Amtsanschluss [88](#)
 OpenScape Business X3R:Baugruppen-Steckplätze [86](#)
 OpenScape Business X3R:Sichtkontrolle durchführen [99](#)
 OpenScape Business X3R:Wandmontage [76](#)
 OpenScape Business X3W
 Baugruppeninstallation [52](#)
 OpenScape Business X3W
 Anschlusskabel [48](#)
 Baugruppen-Steckplätze [49](#)
 Montage [40](#)
 Montagestandort [32](#)

- Netzspannungsanschluss (nur für USA/Kanada) [35](#)
- Verbindungskabel zum externen Hauptverteiler [281](#)
- Wandmontage [40](#)
- Werkzeuge und Hilfsmittel [31](#)
- OpenScape Business X3W
 - LAN-Port [53](#)
 - Störaussendungen [65](#)
 - WAN-Schnittstelle [53](#)
- OpenScape Business X3W: Anschluss von Telefonen und Geräten [58](#)
- OpenScape Business X3W:Amtsanschluss [54](#)
- OpenScape Business X3W:Sichtkontrolle durchführen [70](#)
- OpenScape Business X5R
 - 19"-Schrankmontage [74](#)
 - Abschirmblende für Baugruppe [88](#)
 - Baugruppeninstallation [87](#)
 - Montage [73](#)
 - Montagestandort [32](#)
- OpenScape Business X5R: Anschluss von Telefonen und Geräten [92](#)
- OpenScape Business X5R:Amtsanschluss [88](#)
- OpenScape Business X5R:Baugruppen-Steckplätze [87](#)
- OpenScape Business X5R:Sichtkontrolle durchführen [99](#)
- OpenScape Business X5R:Wandmontage [76](#)
- OpenScape Business X5W
 - Störaussendungen [65](#)
- OpenScape Business X5W
 - Amtsanschluss [54](#)
 - Anschlusskabel [48](#)
 - Baugruppeninstallation [52](#)
 - LAN-Port [53](#)
 - Montage [40](#)
 - Montagestandort [32](#)
 - Netzspannungsanschluss (nur für USA/Kanada) [35](#)
 - Steckplätze [50](#)
 - Verbindungskabel zum externen Hauptverteiler [281](#)
 - WAN-Schnittstelle [53](#)
 - Wandmontage [40](#)
 - Werkzeuge und Hilfsmittel [31](#)
- OpenScape Business X5W: Anschluss von Telefonen und Geräten [58](#)
- OpenScape Business X5W:Sichtkontrolle durchführen [70](#)
- OpenScape Business X8
 - Abschirmkappe für Baugruppe [131](#)
 - Baugruppeninstallation [129](#)
 - Verbindungskabel zu MDFU-E [138](#)
 - Vornehmen einer Sichtprüfung [154](#)
- OpenScape Business X8
 - 19"-Schrankmontage [107](#)
 - Amtsanschluss [142](#)
 - Anschluss- oder Abschirm-Panel [135](#)
 - Backplane [132](#)
 - Freistehende Montage [102](#)
 - Montage [102](#)
 - Montagestandort bei 19"-Schrankmontage [33](#)
 - Montagestandort bei freistehender Montage [31](#), [33](#)
 - PCM-Highways in der Basisbox [126](#)
 - PCM-Highways in der Erweiterungsbox [127](#)

- Schutzerdung [113](#)
- Verbindungskabel zum Patch-Panel [139](#)
- Verbindungskabel zum S0-Patch-Panel [139](#)
- Zeitmultiplexkanäle der Peripheriebaugruppen [128](#)
- OpenScape Business X8: Anschluss von Telefonen und Geräten [146](#)
- OpenScape Business X8: Systembox verschließen [156](#)

P

- Patch-Panel [110](#)
 - Montage [113](#)
 - Schutzerdung [113](#)
- PCM-Highways
 - Basisbox [126](#)
 - Erweiterungsbox [127](#)

R

- Recycling [23](#)
- Remote-Zugang
 - einschalten, über Internet-Zugang mit fester IP-Adresse [253](#), [253](#), [255](#)
 - über Internet-Zugang mit fester IP-Adresse einschalten [250](#)
- Rufnummernplan [185](#)

S

- Schutzerdung
 - Hauptverteiler MDFU [41](#)
 - X3R [77](#)
 - X3W [41](#)
 - X5R [77](#)
 - X5W [41](#)
- Sicherheitshinweise [13](#)
- Sicherheitshinweise für Australien [17](#)
- Sicherheitshinweise für Brasilien [18](#)
- Sicherheitshinweise für Kanada [21](#)
- Sicherheitshinweise für USA. [18](#)
- Steckplätze in der Basisbox [122](#)
- Steckplätze in der Erweiterungsbox [123](#)
- Störaussendung [27](#)

T

- Themen, Arten [12](#)

U

- Unfall melden [22](#)

V

- Verhalten im Notfall [22](#), [22](#)
- Verkabelung für LAN- und WAN-Anschlüsse [24](#)

Versorgungsstromkreis und Anschluss

OpenScape Business S [24](#)

OpenScape Business UC Booster Server [24](#)

W

Warnhinweise [13](#)

Gefahr [14](#)

Hinweis [16](#)

Vorsicht [15](#)

Warnung [14](#)

Z

Zeitmultiplexkanäle [128](#)

